GUIDE SPECIFICATION

VERSION 1.0.2.3

Network Harbor, Inc. is the developer of the Lions Gate™ Identity Management System (IDMS). The company is a Microsoft Certified Development Partner and a Microsoft Early Innovator parent, as well as a participating member of both the National Institute of Standards and Technology, and the Armed Forces Communication and Electronics Association. Members of Network Harbor, Inc.'s executive management and development staff have over 20 years of experience in security integration development and 15 years of experience in high capability IDMS development.

The Lions Gate suite of products, to be released this year, is the product of over two years of development, testing and quality assurance. It is designed to meet the robust identity management and visitor management requirements of government including the military and is fully integrated with the PIV and CAC smart cards issued by those agencies. It leverages that card, not only for three factor authenticated logon, but for the digital signing of every transaction performed in the software. It uses FIPS compliant PKI security for information transference, and allows for a consistently pleasant and efficient ultimate end-user (cardholder) experience, as well as allowing our customers to save substantial money, and have increased flexibility and control of their physical access control infrastructure.

For additional information, contact:

Network Harbor, Inc.
5607 South Washington St.
Bartonville, IL 61607
Phone: +1 309.633.9118
Web: http://www.networkharbor.com
Email: sales@networkharbor.com

Identity Management System for U.S. Government Agencies

PART 1 – GENERAL

1.01 SUMMARY

A. System unites all information related to Physical Access Security for all personnel under one system including (but not limited to):
   a. Biographic information such as name, date of birth, state and country of birth, country of citizenship, height, weight, gender race, eye color, hair color, and Social Security Number (note that access to these fields to view or edit can be maintained by administrators).
   b. Service Branch and Rank information for military personnel including date of rank and lineal number for naval personnel.
   c. Security Clearance and access level information including SCI, Special, and Collateral clearances.
   d. Aliases such as prior names due to marriage.
   e. Billet / Employment information.
   f. All information for badges including the public certificates from PIV and CAC (for periodic revalidation).
   g. Transgressions of the Continuous Evaluation Program, and reports and adjudication of those transgressions.
   h. Physical key (think normal house or door key) management.
   i. Training (security, safety and other types of training that might be pertinent to physical or logical access).
   j. Biometrics including the templates stored on the PIV or CAC and those captured through the software.
   k. Person contact information such as phone, email, and address information.
   l. The person's contacts (spouse, emergency, etc.).
   m. Notes pertaining to the person.
   n. Source documents such as Driver's License, Passport, and other documents that may have been captured, for instance, for visitors.
   o. Rich Text Documents (Word type documents), Spreadsheets (Excel type documents), and Scanned Documents which can be associated with almost every other element mentioned above.
   p. Background Investigations and their results.
   q. Minor violations of security policy.
   r. Vehicles, and
   s. Parking Tags

B. System unites all Command / Agency / Contractor information under one system including (but not limited to):
    a. Command / Agency / Contractor
        i. Name and Short Name (for legacy credential placement).
        ii. Parent (Command / Agency / Contractor).
        iii. Agency / Business Type
        iv. Status of Command / Agency / Contractor
        v. Identifier and billing number for integration with other systems.
        vi. Contact information such as phone, email and addresses (general).
        vii. Specific contact names along with their contact information and the type of contact.
        viii. Vehicles
        ix. Parking
        x. Insurance information
        xi. Divisions of the Command / Agency / Contractor and their information including (but not limited to):
            1. Division Name and Facility the division falls under (physical base location).
            2. Type and Status of division.
            3. Identifier and Billing Identifier.
            4. Job Titles / Billets that the division has been assigned including (but not limited to) the following information for each billet:
                a. Name of the billet,
                b. Default Legacy badge type to be assigned to billet,
                c. Contract (if company is a contractor),
                d. Default physical access control system access to be assigned to personnel in that billet during onboarding automatically (if requirements are met) including:
                    i. Readers,
                    ii. Access Codes,
                    iii. Access Groups, and
                    iv. Time Codes.
            5. Sponsors associated with Division (that is personnel who may authorize access within the Division).
            6. Employees currently associated with Division.
            7. Vehicles, Insurance, and Parking.
C. System is highly integrated with Government PIV and CAC smart cards using them for at least the following features:
    a. Data harvesting of information from the PIV or CAC during on-boarding (if the person is not a transfer from another Lions Gate facility).
    b. Three factor logon (with full certificate validation in high security mode).
    c. On-Card digital signing of every transaction in the system.

    d. Private key challenge – response.

D. The software allows business rules management for the assignment of billets, access codes, readers, access groups, and legacy credential types including (but not limited to):
    a. Required background investigations,
    b. Required training,
    c. Command / Agency / Contractor requirements (perhaps only personnel assigned to a specific command may have the credential, access code, etc. assigned),
    d. Insurance,
    e. Security Clearance,
    f. SCI Clearance,
    g. Special Clearance, or
    h. Collateral Clearance.

E. The system is highly secure and transactions are non-reputable. Each transaction is:
    a. Digitally signed by the PIV or CAC of the user performing the transaction,
    b. Digitally signed by a proprietary method, and
    c. If possible a screenshot of the software is captured at the moment the transaction is performed and stored in an encrypted format in the database.
    d. The On-Card hash signature and public key are recorded in the database for each transaction for independent verification and forensic evaluation.

F. Since all transactions are tracked, the system allows significant management capability such as efficiency analysis of users, and the identification of processing bottlenecks can be easily performed.

G. The system has a highly capable financial module covering such items as credential issuance, minor violation adjudication, fees associated with physical key management, and other items. The system can work with a cash drawer and receipt printer if one is available for these purposes.

H. The system has advanced error logging including:
    a. Storing the error in an encrypted error log, and
    b. Storing an encrypted screenshot of the software at the time of the error if possible.

I. The system allows sophisticated user security including (but not limited to) the following:
    a. What menu items and short cuts that the user has access to.
    b. What tabs on the personnel screen the user has access to, and which he or she may edit.
    c. What controls on the home tab (demographic and basic information) the person has access to and which can be edited (like the user name and password, Social Security Number, etc.).
    d. What facilities that the user has access to.
    e. What access views the user has access to (both of these last two (facility and access view)) determine what access codes and personnel a user can see, and in the case of access views, even if they span multiple facilities. For instance, a special or command element may wish its access codes and personnel invisible to all but a

select group of system users, even if these personnel are spread over multiple facilities. Lions Gate can enable that functionality.

f. What reports the user can access, and whether the user can edit the report design.
g. What background investigations the user can view (if the person has them assigned), and whether the user can initiate and edit the background investigation. It is a good idea to split the functions of initiating and finalizing background investigations.

1.02 REFERENCES

A. Abbreviations
   a. AES – Advanced Encryption Standard
   b. CAC – Common Access Card (Smart Card issued to military personnel, civilians working for the Department of Defense, and select government contractors working for the Department of Defense).
   c. DoD – Department of Defense.
   d. FIPS – Federal Information Processing Standard
   e. HSPD – Homeland Security Presidential Directive
   f. LAC(S) – Logical Access Control (Logical Access Control System)
   g. PACS – Physical Access Control System
   h. PIV – Personal Identity Verification (Smart Card issued to non-military government personnel and select government contractors).
   i. PKI – Public Key Infrastructure
   j. SHA – Secure Hash Algorithm

1.03 SUBMITTALS

A. Informational Submittals
   a. Product Data – Manufacturer's printed or electronic data sheets.
   b. Manufacturer's instructions.
B. Closeout Submittals
   a. Warranty documentation
   b. Manufacturer's installation, configuration, and operation manuals and html help.
   c. Manufacturer's compliance and performance test reports
   d. Software – Copy of all applicable operating software
   e. Recommended spare parts list

1.04 QUALIFICATIONS

A. Manufacturer – Shall have a minimum of five (5) years' experience in the PACS security industry.
B. Installers
    a. Installers shall be authorized by the Manufacturer to install, configure and commission the IDMS.
    b. Three years of experience installing at least one of the Manufacturer's products.
C. Project Manager – Certified by the Manufacturer to manage the IDMS installation.

1.05 WARRANTY

A. Manufacturer shall provide a limited three (3) Year Warranty for all software products to be free of defects in material and workmanship subject to license agreement terms and conditions. *
B. Manufacturer shall offer the option to upgrade its standard warranty to a limited four (4) or five (5) year warranty. *
C. Manufacturer shall offer Software Assurance Agreement option to include availability of software updates and support.

* Warranty does not include software support or free upgrades other than that required to correct defects under the terms of the warranty in effect and license agreement.

1.06 LICENSING

A. The Contractor shall procure all necessary licenses, including devices, portals, and special features, from the Manufacturer.

END OF SECTION

2.01 EQUIPMENT

A. Manufacturer: Network Harbor, Inc.

5607 South Washington Street

Bartonville, IL 61607

Phone: +1 309.633.9118

Web: http://www.networkharbor.com

E-mail: sales@networkharbor.com

B. Model(s): Lions Gate Enterprise

C. Alternatives: None

2.02 IDMS REQUIREMENTS – SECURITY

IMPORTANT – Any response that fails to meet, or takes exception to, one or more of the requirements of this section shall be disqualified.

The IDMS shall have the following security features at a minimum:

A. The IDMS shall use the PIV / CAC for three factor (card, card pin, biometric) logon to the software for users.
B. The IDMS shall enable a high security and a low security logon to the software.
    a. In high security mode the following additional functions shall be performed:
        i. A long chain certificate validation shall be performed on the certificates on the card.
        ii. A private key challenge and response validation shall be performed on at least one of the card certificates.
        iii. The administrator shall have the option of running certificate validation through an SCVP server.
    b. In low security mode, the three factor authentication only shall be performed.
C. The IDMS shall store a before and after XML image of each and every transaction performed in the system, along with, if possible, and encrypted image of the software at the time the transaction was performed. (Note that the before XML image will be blank for records that are created, and the after XML image will be blank for records that are deleted).
D. The IDMS shall create a tamper-proof digital signature of the before and after images.
E. The IDMS shall perform an on-card PIV/CAC digital signature of the:
    a. After XML image in case of record creation.

b. After XML image in case of record update.
c. Before XML image in case of record delete.
d. The public key of the on-card certificate, along with the signature hash shall be stored in the database along with the record of the transaction for independent verification.

F. All of these features shall be made readily available in the software for a system user to see when they are looking at records so as to show a complete history of the record from birth onward (depending on the archiving requirements and data capacity of the client system of course).
G. An administrator may see a transaction list with all of these features apparent, when he or she views a user's record to enable the administrator to keep track of exactly what the users are doing in the system.

2.03 IDMS REQUIREMENTS – Personnel Attributes

IMPORTANT – Any response that fails to meet, or takes exception to, two or more of the requirements of this section shall be disqualified with the exception of the Continuous Evaluation Program (CEP) which, if the response fails to meet or takes exception to, shall be disqualified on that basis alone.

The IDMS shall, at a minimum, track the following attributes for a personnel (cardholder) record:

A. Basic identifying and biographical data such as (note administrators may configure each of these fields for viewing or updating on a user-type basis so that personally identifiable information is kept on a need to know basis):
    a. Name (first, middle, last)
    b. User Name and Password
    c. Date of Birth
    d. Country and (if the United States), State of Birth.
    e. Country of Citizenship
    f. Height and Weight
    g. Gender
    h. Race
    i. Eye Color and Hair Color
    j. Social Security Number
    k. Service Branch and Rank (military or can be used for civilians GS, GM, ES type ratings also) including date of rank for Army and Air Force, and Lineal Number for Navy and Marine Corps personnel.
    l. Security Clearance, Current Access Level (which may be different).
    m. The IDMS shall be capable of displaying data for an unlimited number of the following attributes for a personnel (cardholder) record.
        i. SCI, Special, and Collateral Security Clearances held.
            1. The following additional documents shall be available to be associated with any SCI, Special, and Collateral Clearances held:
                a. Scanned Documents
                b. Rich Text (Word Type) (Edit Capability)

c. Spreadsheets (Edit Capability)

ii. Aliases (normally used for maiden or prior married names)
   1. The following additional documents shall be available to be associated with any Aliases:
      a. Scanned Documents
      b. Rich Text (Word Type) (Edit Capability)
      c. Spreadsheets (Edit Capability)

iii. Billet or Employment Job Titles information including:
   1. An association with a contract vehicle for contractors on base.
   2. The Access (Access Groups, Access Codes, and Readers) that were assigned to the individual as a result of his or her billet / job title assignment.
   3. The following additional documents shall be available to be associated with any Billet or Employment Job Titles held:
      a. Scanned Documents
      b. Rich Text (Word Type) (Edit Capability)
      c. Spreadsheets (Edit Capability)

iv. Badge records which shall contain:
   1. In the case of PIV/CAC records the following data shall be displayed:
      a. FASC-N (broken out into its constituent elements).
      b. Last Name, First Name, and Middle Name
      c. Gender
      d. Date of Birth
      e. Issue Date
      f. Expiration Date
      g. The public portion of the Card Authentication, PIV Authentication, and Digital Signing Certificate along with a visual means of determining the status (Verified) of the certificates.
      h. The Access Groups, Access Codes, and Readers assigned to the credential
      i. The credential number (randomly assigned, prox number, badge type, expiration date, user assigned badge number, the badge status, the status date.
      j. The authorized signer (command or company sponsor), and the authorized co-signer (base or agency security manager approval).
      k. The pin number (for legacy credential types)
      l. Whether the badge has timed override, or executive privilege capability.
      m. The ability to associate the following additional documents with a badge:

i. Scanned Documents
ii. Rich Text Documents (with edit capability)
iii. Spreadsheet (with edit capability)

v. Records of transgressions of the Continuous Evaluation Program (CEP), the investigation and counseling sessions, and the final adjudication of these transgressions including but not limited to:
    1. The incident number (system determined).
    2. The incident date.
    3. The incident status (cannot be set to final until all associated personnel have been adjudicated).
    4. The initiator (incident may be self-reported or initiated).
    5. The incident location.
    6. An initial description of the incident.
    7. The following additional documents shall be available to be associated with any CEP:
        a. Scanned Documents
        b. Rich Text (Word Type) (Edit Capability)
        c. Spreadsheets (Edit Capability)
    8. Any personnel associated with the incident, and a quick view of their record containing the following information:
        a. Portrait
        b. Name (last, Middle, First)
        c. SSN
        d. User Name
        e. Clearance
        f. Access Level
        g. Service Branch
        h. Rank
        i. The reason they were associated with the CEP (primary accused, witness, etc.)
        j. The adjudication (for accused personnel).
        k. The adjudication date and a Text note for the final adjudication.
        l. The following additional documents shall be available to be associated with any CEP associated personnel:
            i. Scanned Documents
            ii. Rich Text (Word Type) (Edit Capability)
            iii. Spreadsheets (Edit Capability)
    9. The Violation Categories (CEP rules that were violated – there are frequently multiple rule violations arising out of a single incident) including:
        a. Rule Violated.
        b. Violation Date.

c. Rational behind the association (why the incident broke that rule).
d. The following additional documents shall be available to be associated with any CEP associated violation category:
    i. Scanned Documents
    ii. Rich Text (Word Type) (Edit Capability)
    iii. Spreadsheets (Edit Capability)

10. The interim reports including counseling sessions associated with the CEP incident including the following data:
    a. Report Type
    b. Report Date
    c. Entering User
    d. The following additional documents shall be available to be associated with any CEP report:
        i. Scanned Documents
        ii. Rich Text (Word Type) (Edit Capability)
        iii. Spreadsheets (Edit Capability)

vi. Physical Key Management – The software shall have the capability of maintaining records of physical keys (those keys used to open doors that are not controls by an underlying PACS, but instead are secured through the use of mechanical, and smart, key locks) issued to personnel including:
    1. the credential the keys are associated with,
    2. the key type issued,
    3. the serial number of the issued key,
    4. the status of the key, and
    5. the status date.
    6. In addition, the software shall provide a means of designating a "Key" user who shall have a touch sensitive interface (if a touch sensitive monitor is provided) to perform the following functions:
        a. Key Issuance
        b. Key Transfer between Personnel
        c. Key recovery
    7. The following additional documents shall be available to be associated with any Key assignment:
        a. Scanned Documents
        b. Rich Text (Word Type) (Edit Capability)
        c. Spreadsheets (Edit Capability)

vii. Records of Training Received – The software shall be capable of recording the training a cardholder has received, including (but not limited to) the following:
    1. the course taken,
    2. the training date,
    3. the instructor performing the training,

4. an indicator that the person received a passing grade,
5. the score or grade for the course,
6. whether the training has been invalidated (usually as a result of a violation of policy indicating the training should reoccur),
7. the date normal refresher training should occur, and
8. the certificate no (if a certificate was issued).
9. The following additional documents shall be available to be associated with any training record:
    a. Scanned Documents
    b. Rich Text (Word Type) (Edit Capability)
    c. Spreadsheets (Edit Capability)

viii. Biometrics – The software shall be capable of capturing fingerprint images for each cardholder and shall additionally be capable of performing the following functions:

1. Creation of an ANSI-378 template.
2. Displaying the fingerprint along with all identified points circled along with the type of point (bifurcation, ridge ending, or other).
3. Displaying the ANSI-378 header information (format ID, version, record length, width, height, horizontal resolution, etc.).
4. Displaying the fingerprint view header information.
5. Displaying template data for each minutiae in the template including (name, type, x-coordinate, y-coordinate, angle, and quality).
6. The following additional documents shall be available to be associated with any biometric record:
    a. Scanned Documents
    b. Rich Text (Word Type) (Edit Capability)
    c. Spreadsheets (Edit Capability)

ix. Address – The software shall be capable of storing address (domicile, mailing, etc.) for each cardholder including the following information:

1. the address type,
2. the street address (unlimited in length),
3. the city,
4. the state,
5. postal code,
6. country, and
7. county (which shall be available in a pull down list box once the state has been chosen).
8. The following additional documents shall be available to be associated with any address record:
    a. Scanned Documents
    b. Rich Text (Word Type) (Edit Capability)
    c. Spreadsheets (Edit Capability)

x. Email Address – The software shall be capable of storing email addresses (personal, business, etc.) for each cardholder including the following information:
    1. the email type, and
    2. the email address.
    3. The following additional documents shall be available to be associated with any email address record:
        a. Scanned Documents
        b. Rich Text (Word Type) (Edit Capability)
        c. Spreadsheets (Edit Capability)

xi. Phone Numbers – The software shall be capable of storing phone numbers (personal, business, mobile, fax, etc.) for each cardholder including the following information:
    1. the phone type, and
    2. the phone number.
    3. The following additional documents shall be available to be associated with any email address record:
        a. Scanned Documents
        b. Rich Text (Word Type) (Edit Capability)
        c. Spreadsheets (Edit Capability)

xii. Contacts – The software shall be cable of storing contacts (spouse, emergency, etc.) for each cardholders record including:
    1. the contact type,
    2. the contacts:
        a. last name,
        b. first name, and
        c. middle name
    3. address information for the contact just as in section ix above,
    4. email address information for the contact just as in section x above, and
    5. phone number information for the contact just as in section xi above.
    6. The following additional documents shall be available to be associated with any contact record:
        a. Scanned Documents
        b. Rich Text (Word Type) (Edit Capability)
        c. Spreadsheets (Edit Capability)

xiii. Notes – The software shall be capable of storing notes for each cardholder including (but not limited to) the following information:
    1. note type, and
    2. note text.
    3. The following additional documents shall be available to be associated with any note record:
        a. Scanned Documents

b. Rich Text (Word Type) (Edit Capability)
c. Spreadsheets (Edit Capability)

xiv. Source Documents – The software shall be capable of storing source documents (those documents used to verify identity and right to work before access is granted or credential issuance for non-PIV or CAC cardholders) including (but not limited to) the following information:
1. source document type,
2. document number,
3. expiration date,
4. issuing state, and or
5. issuing country.
6. The following additional documents shall be available to be associated with any source document record:
a. Scanned Documents
b. Rich Text (Word Type) (Edit Capability)
c. Spreadsheets (Edit Capability)

xv. Rich Text Documents – In addition to all the other areas where rich text (Microsoft Word type documents), can be stored for a cardholder record, there shall be a general place for the record where these documents may also be recorded.
1. These documents, as in other places shall be editable.
2. Changes to these documents shall be recorded and signed on-card by the users PIV or CAC as normal.
3. The document shall be displayed when on the record, and a thumbnail shall be displayed in the grid for easy visual selection by the user.

xvi. Spreadsheet Documents – In addition to all the other areas where spreadsheet (Microsoft Excel type documents), can be stored for a cardholder record, there shall be a general place for the recording of these documents.
1. These documents, as in other places shall be editable.
2. Changes to these documents shall be recorded and signed on-card by the users PIV or CAC as normal.
3. The document shall be displayed when on the record, and a thumbnail shall be displayed in the grid for easy visual selection by the user.

xvii. Scanned Documents – In addition to all the other areas where scanned documents may be associated with a cardholder record, there shall be a general place for the recording of these documents.
1. The document shall be displayed as a PDF when on the record with the capability of “Save As”, “Print”, “Previous” (page), “Next” (page), “Zoom Out”, “Zoom In”, and “Zoom” (percentage), and a thumbnail of each shall be displayed in the grid for easy visual selection by the user.
2. The software shall be capable of a TWAIN scanned document capture by a scanner with this type of device driver.

xviii. Background Investigations – The software shall be capable of recording background investigations and checks performed on the cardholder including (but not limited to) the following information:
    1. background type,
    2. the initial status,
    3. the reason for performing the check (required for billet, access code, etc.)
    4. the date the check was initiated,
    5. the date the results were returned,
    6. the case no,
    7. the return code,
    8. the final status of the check,
    9. who authorized this final status, and
    10. notes.
    11. The following additional documents shall be available to be associated with any background check record:
        a. Scanned Documents
        b. Rich Text (Word Type) (Edit Capability)
        c. Spreadsheets (Edit Capability)

xix. Violations of Policy – The software shall be capable of recording violations of policy not covered by the CEP above (these usually constitute minor violations of policy to be determined by the administrator) including the following information:
    1. violation type,
    2. violation number,
    3. credential the violation was associated with,
    4. violation date,
    5. violation issuer,
    6. entry date,
    7. location of violation,
    8. disposition (adjudication),
    9. indicators to display:, and
        a. whether a fine was charged,
        b. whether the credential was confiscated, and
        c. if retraining is required
    10. notes.
    11. The following additional documents shall be available to be associated with any violation record:
        a. Scanned Documents
        b. Rich Text (Word Type) (Edit Capability)
        c. Spreadsheets (Edit Capability)

xx. Trainer – If the person has been identified as a trainer (instructor) that can teach courses and provide training as defined in the system, the software shall be capable of recording:
    1. the course the trainer is qualified to teach, and
    2. whether he or she is currently actively able to teach this course.
    3. The following additional documents shall be available to be associated with any violation record:
        a. Scanned Documents

xxi. Authorized Signers – If the person has been identified as an authorized signer or co-signer they may not be allowed to assign all access codes, access groups, or readers based on their authorization. The software shall allow the administrator to designate, if this is a part of policy, what codes the signer shall be authorized to approve access for.
    1. The following additional documents shall be available to be associated with any violation record:
        a. Scanned Documents
        b. Rich Text (Word Type) (Edit Capability)
        c. Spreadsheets (Edit Capability)

xxii. Vehicle Access – The software shall be capable of associating a vehicle access approval with a cardholder record which shall have the following information:
    1. vehicle type (car, truck, etc.),
    2. vehicle year,
    3. make and model,
    4. color,
    5. registration number, and
    6. area of access.
    7. The following additional documents shall be available to be associated with any vehicle record:
        a. Scanned Documents
        b. Rich Text (Word Type) (Edit Capability)
        c. Spreadsheets (Edit Capability)

xxiii. Parking Tags – The software shall be capable of recording the issuance of parking tags including the following information:
    1. parking area assigned,
    2. permit number,
    3. tag number,
    4. issuing state, and
    5. billet or job title to which this tag applies.
    6. The following additional documents shall be available to be associated with any vehicle record:
        a. Scanned Documents
        b. Rich Text (Word Type) (Edit Capability)

c. Spreadsheets (Edit Capability)

xxiv. Insurance – The software shall be capable of recording insurance policies that a cardholder may have and which are pertinent to agency needs including the following information:

1. type of policy,
2. carrier,
3. policy number,
4. expiration date,
5. activation date,
6. contact name,
7. contact phone, and
8. an indicator if the policy is active.
9. The following additional documents shall be available to be associated with any insurance record:
    a. Scanned Documents
    b. Rich Text (Word Type) (Edit Capability)
    c. Spreadsheets (Edit Capability)

2.04 IDMS REQUIREMENTS – Agencies / Commands / Company Information

A. Overview

As a practical matter, a military base or government agency facility usually contains multiple commands or agencies of the government, each of which may have multiple sub-commands with billets assigned. In addition, the base or agency facility often has civilian contracting agencies, again with multiple divisions and their assigned job titles.

Since it is anticipated that the assignment of a billet or job title to a person requires the same access to PACS systems as other or previous holders of the same billet, access codes, groups, and readers shall be assignable to the billet / job title so that during on-boarding access may be assigned in an efficient manner that will reduce the possibility of over or under assigning access to an individual.

B. Requirements

a. The software shall be capable of supporting the following command/ agency / company data elements at a minimum:
    i. command / agency / company name,
    ii. parent (superior) command / agency / company
    iii. short name (for display on a software produced legacy or visual indication badge),
    iv. type of command / agency / company (U.S. Government Agency, Contractor, Base Operator, etc.),
    v. status,
    vi. identifying number, and

vii. billing number.

b. For each command / agency / company an unlimited number of the following attributes shall be available to be stored.
   i. Address – The software shall be capable of storing address (domicile, mailing, etc.) for each command / agency / company including the following information:
      1. the address type,
      2. the street address (unlimited in length),
      3. the city,
      4. the state,
      5. postal code,
      6. country, and
      7. county (which shall be available in a pull down list box once the state has been chosen).
      8. The following additional documents shall be available to be associated with any address record:
         a) Scanned Documents
         b) Rich Text (Word Type) (Edit Capability)
         c) Spreadsheets (Edit Capability)
   ii. Email Address – The software shall be capable of storing email addresses (personal, business, etc.) for each command / agency / company including the following information:
      1. the email type, and
      2. the email address.
      3. The following additional documents shall be available to be associated with any email address record:
         a) Scanned Documents
         b) Rich Text (Word Type) (Edit Capability)
         c) Spreadsheets (Edit Capability)
   iii. Phone Numbers – The software shall be capable of storing phone numbers (personal, business, mobile, fax, etc.) for each command / agency / company including the following information:
      1. the phone type, and
      2. the phone number.
      3. The following additional documents shall be available to be associated with any email address record:
         a) Scanned Documents
         b) Rich Text (Word Type) (Edit Capability)
         c) Spreadsheets (Edit Capability)
   iv. Contacts – The software shall be cable of storing contacts (spouse, emergency, etc.) for each command / agency / company record including:
      1. the contact type,
      2. the contacts:

1. last name,
2. first name, and
3. middle name

3. address information for the contact just as in section ix above,
4. email address information for the contact just as in section x above, and
5. phone number information for the contact just as in section xi above.
6. The following additional documents shall be available to be associated with any contact record:
    1. Scanned Documents
    2. Rich Text (Word Type) (Edit Capability)
    3. Spreadsheets (Edit Capability)

v. Notes – The software shall be capable of storing notes for each command / agency / company including (but not limited to) the following information:

1. note type, and
2. note text.
3. The following additional documents shall be available to be associated with any note record:
    1. Scanned Documents
    2. Rich Text (Word Type) (Edit Capability)
    3. Spreadsheets (Edit Capability)

vi. Vehicle Access – The software shall be capable of associating a vehicle access approval with a command / agency / company record which shall have the following information:

1. vehicle type (car, truck, etc.),
2. vehicle year,
3. make and model,
4. color,
5. registration number, and
6. area of access.
7. The following additional documents shall be available to be associated with any vehicle record:
    a) Scanned Documents
    b) Rich Text (Word Type) (Edit Capability)
    c) Spreadsheets (Edit Capability)

vii. Parking Tags – The software shall be capable of recording the issuance of parking tags including the following information:

1. parking area assigned,
2. permit number,
3. tag number,
4. issuing state, and
5. billet or job title to which this tag applies.
6. The following additional documents shall be available to be associated with any vehicle record:

a) Scanned Documents
b) Rich Text (Word Type) (Edit Capability)
c) Spreadsheets (Edit Capability)

viii. Insurance – The software shall be capable of recording insurance policies that a command / agency / company may have and which are pertinent to agency needs including the following information:

1. type of policy,
2. carrier,
3. policy number,
4. expiration date,
5. activation date,
6. contact name,
7. contact phone, and
8. an indicator if the policy is active.
9. The following additional documents shall be available to be associated with any insurance record:
    a) Scanned Documents
    b) Rich Text (Word Type) (Edit Capability)
    c) Spreadsheets (Edit Capability)

ix. Financial

1. Overview – Because both government agencies and contractors may inhabit common facility, and because there may be reason to charge the contractors for items, and because these charges may be negotiated as part of a contractual agreement and thus may be different for each contractor, the software must support a financial module capable of supporting these requirements. For each item identified to be purchasable through the system (or fine accessed or badge issuance charge identified in the system), a fee that can be command / agency / company and division attributable must be able to be set. Therefore a financial tab must be available in the company view to display, and edit, this information including:
    a) The rate that will be charged for the item or fee, and
    b) The charge type that will be entertained (charge to contractor or pay when issued).

x. Divisions of Commands / Agencies / Companies

1. Overview – Each of the Commands / Agencies / Companies may have an unlimited number of divisions. Divisions are assigned to a facility so shall be used when a command / agency / or company spans multiple facilities so as to be able to designate what facility the billet pertains to and whether that person can be viewed by a user (user views can be segregated by facility).
2. The software shall be capable of supporting the following basic information for each division:
    a) division name,

b) facility assigned to,
c) type of division (should follow company but does not have to),
d) status of division,
e) division number (assigned automatically),
f) billing ID, and
g) whether the division is designated as a co-signing authority for the company.
h) In addition to these items, the software shall be capable of supporting an unlimited number of the following additional attributes:
    a. Addresses as in the company section 2.04 (B) (b) (i) above,
    b. Email address as in the company section 2.04 (B) (b) (ii) above,
    c. Phone Numbers as in the company section 2.04 (B) (b) (iii) above,
    d. Contacts as in the company section 2.04 (B) (b) (iv) above,
    e. Notes as in the company section 2.04 (B) (b) (v) above,
    f. Vehicle Access as in the company section 2.04 (B) (b) (vi) above,
    g. Parking Tags as in the company section 2.04 (B) (b) (vii) above,
    h. Insurance as in the company section 2.04 (B) (b) (viii) above,
    i. Financial as in the company section 2.04 (B) (b) (ix) above, and
    j. Billet / Job Title Information – The software shall be capable of supporting an unlimited number of billets / job titles for each division. Information stored for the billet shall include:
        i. Description or title,
        ii. Default legacy or visual identification badge associated with the billet,
        iii. Threat level,
        iv. Contact (if the division has been identified as a contractor),
        v. The default access codes, access groups, and readers that will be assigned to personnel onboarding with this billet.

2.05 IDMS REQUIREMENTS – User Setup and Additional Security Elements

A. Overview

The government has need of software that is multi-facility capable, but can segregate the ability of a user to see cardholder records to those facilities that the administrator has determined that the user should have access to. In addition, there may be some access codes, groups, and readers that the users of the system should be segregated from unless they require the ability to see these codes (high security and classified area access for instance).

Therefore it is an absolute requirement that the software be able to support this functionality and no exceptions may be made to this requirement.

The software shall be capable of:

1. Allowing the administrator to maintain a list of facilities,
2. To assign each of these facilities as public / private key pair for the encryption of data in transit between facilities. The private key shall be created in SQL server with a randomly generated password so it can be backed up routinely as a part of local facility data backup.
3. The software shall provide a central windows service where facilities created by the local administrator are sent to so that they may be approved (VPN, firewall, certificates, and other IT related issues will have to be done before a brand new facility (no previous facilities created from that IP address) is created). Once approved, they will be listed in the drop down box so that they can be chosen in the Lions Gate Government Kiosk.
4. An unlimited number of PACS shall be associated with each facility though these connectors may be separately licensed.
5. For each PACS the system shall automatically retrieve the access codes, readers, and (if available) time codes from the system to be made available to be assigned in the software.
6. The administrator may create “Access Groups” made up of access codes and readers from one or more access control systems spanning one or more facilities. This provides a convenient way of grouping commonly associated access together regardless of underlying PACS capabilities.
7. Access codes, groups, and readers are assigned to an access view by the administrator.
8. For each user of the system, the administrator may determine what facilities and access views the users has access to.
    a. Assignment of a facility determines cardholder access through assigned billet. If the cardholder has a billet assigned that is within the ones assigned to a user, the user can see the cardholder. The user may not see the cardholder if all the billets he or she has assigned fall outside those assigned to a user. Only one billet correlation is required so that the user can see the cardholder record (that is if any of the cardholder’s billets are available to the user his or her entire record is available to the user even if there are other billets assigned outside the ones available to the user).
    b. Assignment of an Access View determines access to viewing and assigning access codes, groups, and readers within that view. If the cardholder has access codes, groups, or readers outside the views available to the user, they will still be there, but the user will not be able to view, edit, or delete these codes. In addition, the user will only be able to assign new codes based on those he or she has in their access view(s).
9. Background Investigation Access
    a. The software must support the capability of being able to determine which users may view, initiate, and edit a given background investigation. This is to provide for proper segregation of duties, and security over sensitive matters. This is to be configurable for each type of background investigation (that is a user may see one type of investigation, but be unable to see another). Even if the user cannot see a background investigation,

that investigation will be used when determining if the requirements for an access code, access group, etc. are met before assignment.

b. Any user who may initiate or edit a background investigation type must also be able to view the type (obviously).

10. Report Access
    a. The administrator must be able to configure what reports (created via the built in reporting capabilities of the software), are available to each user and whether the user may edit the report layout.
11. User Type Setup
    a. The software must allow the administrator to setup an unlimited number of user types. Each of these user types may be configurable to determine:
        i. What basic menu structure the user is setup with (administrator, user, operations, key shop, etc.)
        ii. What maintenance tables the user can have access to including
            1. Access control settings
            2. Workstation and global settings
            3. Table maintenance
            4. Financial settings
            5. Government settings
            6. CEP settings,
            7. Company settings,
            8. Etc.
        iii. What cardholder tabs the user has access to and whether they may be edited.
        iv. What controls / information the user has access to on the users Home (basic information) tab and whether they may edit the information including:
            1. User name
            2. Date of Birth
            3. Country of Birth
            4. State of Birth
            5. Country of Citizenship
            6. Height / Weight
            7. Gender
            8. Race
            9. Eye Color
            10. Hair Color
            11. Social Security Number (SSN)
            12. Service Branch
            13. Rank
            14. Security Clearance and Access Level

2.06 IDMS REQUIREMENTS – Search

A. Overview

In addition to finding a cardholder by the information on the Home tab of the cardholder record (such as name, SSN, etc.) the user should be able to find cardholders, commands, applications, etc. through the use of tabbed data (address, phone numbers, vehicle registration, etc.), and biometrics.

Searches of each of the criteria mentioned are an essential part of the software and no exceptions will be granted in complying with this section of the specification.

Therefore the software shall provide the means to search by:

a. Home tab fields including:
    1. Cardholder status
    2. Last name
    3. First name
    4. Middle name
    5. User name
    6. Employee number
    7. Date of birth
    8. Country of birth
    9. State of birth
    10. Country of citizenship
    11. Height / weight
    12. Eye color
    13. Hair color
    14. Gender
    15. Race
    16. Social Security Number (SSN)
    17. Billet, Command, Division
    18. Service Branch and Rank
    19. Clearance Level
    20. Access Level
b. Tabbed Data including:
    1. Vehicle Data
    2. Parking Tag Data
    3. Address
    4. Phone
    5. Email Address
    6. Background Investigations
    7. Training
    8. Source Documents
    9. Keys, and
    10. Biometrics

2.07 IDMS REQUIREMENTS – KIOSK

A. Overview

The command needs a variety of information from incoming onboarding personnel that can either be captured form their PIV or CAC card, or more efficiently and privately, be entered by the cardholder themselves rather than being written on a piece of paper that can be lost or incompletely filled out, our divulged orally to a user and overheard by other personnel negating the privacy of the data.

Therefore Kiosk software shall be provided for the following general purposes:

1. Checking into (onboarding) the duty station.
2. Applying for a visit to this or another facility, and
3. Checking in for a previously approved visit.

B. Onboarding

The software shall:

1. Harvest available information from the PIV or CAC.
2. Allow the user to enter a user name and password, pick their service branch and rank (if not harvested from card), date of rank, and lineal number (if known).
3. Provide their agency email address.
4. Provide any other email addresses they wish to add (personal or business).
5. Provide their primary phone number.
6. Provide any other phone numbers they wish to add (personal or business).
7. Provide their home address.
8. Provide any other addresses they wish to add (mailing or other).
9. Provide at least one emergency contact (spouse or other), and their phone number, email address, and home address.
10. Select their reporting command or agency.
11. Provide two biometric fingerprints, one for a finger on each hand.
12. Provide a legally valid eSignature for the.

By providing this data, the user may be efficiently processed when he gets to the processing office. Upon reporting to the processing office the onboarding cardholder shall be placed in the queue, and his or her application will be automatically pulled up for the user when he or she is pulled off the top of the queue.

The user will then finish the processing of the application and on-boarding, able to review rather than enter the details furnished by the onboarding cardholder resulting in a much shorter, efficient, and higher-tech experience by the cardholder. Selection of his billet shall enable the transference of all applicable access codes, groups, and readers for that billet that the user qualifies for (the ones the cardholder does not qualify for will have to be added after the requirement is met such as training, security clearance addition, etc.).

C. Visitor Application

Only a PIV or CAC cardholder at the local facility may initiate a visitor request. Visitor requests are initiated at the kiosk and can be of two basic types:

a. a request for the PIV or CAC cardholder to visit another facility covered by this software, or
b. a request for a government or civilian person(s) to visit the current facility.
c. Each person included on the visitor request must sign a signing statement and their application with a valid eSignature, and in the case of (b) above, the sponsor (PIV or CAC cardholder initiating the request) must approve each person added individually by eSignature and biometric fingerprint authentication and must additionally approve the overall application.

D. Visitor Application Approval

The KIOSK will produce a random key and symmetrically encrypt the application package for transfer. Then it will encrypt the symmetric key using the public key of the receiving facility. This will ensure that only the receiving facility will be able to decrypt the visit package even if any overlying security (like https transmittal) is compromised.

Once the Receiving Facility has the information, the software shall decrypt the package and place the application into a queue for user approval. The user has to approve both the overall application for the visit, and each of the personnel that appear on the application. Once approved, the personnel are available to be maintained as other cardholders in the system.

PART 3 EXECUTION

3.01 INSTALLERS

A. Contractor personnel shall comply with all applicable state and local licensing requirements
B. Contractor is required to be an authorized product Integrator/Dealer to sell, install, or service products offered by the manufacturer.

3.02 EXAMINATION

A. Network – All network connections between network connected devices integral to the overall system shall be tested for proper levels of performance.
B. Ports – All network ports required for system communications shall be opened and/or configured.
C. Certificates – All certificates needed to facilitate https communication between clients and windows services installed as part of this project must be procured, setup, and tested.
D. Manufacturer shall provide communications port information as required for project configuration.

3.03 PREPARATION

A. Contractor shall verify that all required software and available Windows updates have been installed on both servers and client PC's.
B. Manufacturer shall either provide the software pre-requisites on digital media and/or provide access links for download as required.

C. Manufacturer shall provide all software licenses as procured under the requirements for this project.

3.04 INSTALLATION

A. Contractor shall provide all necessary labor and materials as required to install hardware and software provided by the manufacturer.

B. Manufacturer shall provide complete installation manuals and user manuals for all products provided by the manufacturer.

C. Manufacturer shall provide contractor support as defined in manufacturer authorized dealer agreements.

END