Privacy Impact Assessment
Enterprise Physical Access Control System (ePACS) Applications Toolkit

ePACS Application Toolkit

- Version: 2.0
- Date: April 12, 2011
- Prepared for: USDA OCIO

United States Department of Agriculture

Abstract

The ePACS Applications Toolkit supports USDA compliance efforts for the physical access components of the USDA Homeland Security Presidential Directive 12 (HSPD-12), Federal Information Processing Standard 201-1 (FIPS 201-1), and the Office of Management and Budget (OMB) Memorandum M-11-11.

The ePACS Applications Toolkit is comprised of four applications that: afford USDA a means to centralize the distribution and assessment of mission critical physical access control data at the facility, regional, and national levels of the Department; enable the USDA's asset portfolio to be viewed in a spatial format utilizing GIS technology to facilitate the data access and automated reporting, analysis and decision support tools for USDA site security information; identify, analyze and manage potential risks to USDA infrastructure, assets and systems by allowing security and non-security professionals to perform assessments at facilities with little training.

The ePACS Applications Toolkit provides enterprise infrastructure for USDA to issue credentials and to utilize the PIV (LincPass) or PIV-Alternative (PIV-A) credentials for Physical Access Control Systems (PACS). Overall, the applications provide enhanced and centralized physical security capabilities to USDA critical infrastructure.

The four applications are comprised of the following:

- ePACS (Lenel OnGuard Commercial Off the Shelf {COTS})
- Geospatial Security Information Systems (GeoSIS)
- Personal Identity Verification Alternative (PIV-A)
- Critical Risk Information System (CRIS)

Overview

The ePACS Application Toolkit is owned by the Departmental Management (DM), Office of Homeland Security and Emergency Coordination (OHSEC). The ePACS Application Toolkit is managed by OHSEC and is hosted at the National Information Technology Center (NITC) under an agreement to provide Platform as a Service (PaaS) capabilities.

The purpose of the ePACS Applications Toolkit is to ensure that USDA continues to comply with Federal Regulations by applying a comprehensive program designed to mitigate potential threats to the USDA infrastructure.

The ePACS Applications Toolkit is comprised of four applications that afford USDA a means to centralize the distribution, and assessment of mission critical physical access control data at the facility, regional, and national levels of the Department. Each component within the ePACS Applications Toolkit acts independently to support USDA's efforts to comply with related policies.

The following are descriptions of each application within the ePACS Application Toolkit.

ePACS (Lenel OnGuard)

Lenel OnGuard is a COTS product that provides the required authoritative identity data from the government developed identity management system to interface with the local physical access control systems (PACS).

The overall intent of ePACS is to provide the functionality to disseminate authoritative identity data to all USDA PACS nationwide which includes providing:

- Global Real Time Revocation
- Electronic Authentication
- An Authoritative PACS Database
- Auditable Transactions
- Future Scalability and Cost Savings

This identity data is received from the Office of Chief Information Officer (OCIO), Enterprise Identity Management System (EIMS).

GeoSIS

GeoSIS was developed as an analysis tool that enables the USDA's asset portfolio to be viewed in a spatial format. GeoSIS utilizes GIS technology to facilitate the data access and automated reporting, analysis and decision support tools for USDA site security information. The objectives established for this GeoSIS ensures automated, timely access to mission-critical information at the facility, regional, and national level.

CRIS

CRIS was developed for the purpose of identifying, analyzing and managing potential risks to USDA infrastructure, assets and systems. CRIS operates as a web-based self-assessment tool that is utilized for data collection at the facility level. The result is a centralized repository of vulnerability, threat and asset data in which a risk mitigation strategy is developed. The comprehensive, structured methodology of CRIS provides consistent survey response, asset classification and threat assessment across USDA. CRIS allows security and non-security professionals to perform assessments at facilities with little training.

Personal Identity Verification – Alternative (PIV-A)

The USDA PIV-A card issuance system will be developed to integrate with the existing USDA OCIO Enterprise Entitlement Management System (EEMS) infrastructure. The PIV-A

Card issuance system will provide a streamlined work flow that allows a person to schedule cards for printing and delivery and track the activation of a card. Issued cards will be fully compatible with the logical access (LACS) system that is trusted by the Certifying Authority provided by the USDA OCIO.

Information within the ePACS Application Toolkit is not shared with any outside entities. Rules of Behavior have been established to ensure that authorized users do not make any of the reports or data obtained by the system available to the public. Access to the system can only be obtained by authorization from the Director of OHSEC, and compliance with the USDA Two Factor Authentication system.

Section 1.0 Characterization of the Information

1.1 What information is collected, used, disseminated, or maintained in the system?

Each system under the ePACS Applications Toolkit has its own repository of data and handles the data independently of the other systems.

ePACS generally handles Security Management Information including:

- Physical access card status
- Physical access card category,
- Physical access card expiration date,
- Physical access card holder emergency response responsibilities.

ePACS also stores Personal Identity and Logistics information including:

- First Name
- Last Name
- Middle Name
- Employee Agency
- Employee Department
- Employee Office Address
- Employee Telephone Number
- Employee Federal Agency Smart Credential Number (FASCN)

GeoSIS handles information related to Logistics Management, Public Resources, Facility and Infrastructure Management, Inspections and Auditing. The data includes:

- Attribute Data
- Facility Data
- Facility Director Name, Title, Contact Information
- Employee Name, Title, Contact Information

The CRIS application handles data associated with Public Resources, Facility and Infrastructure Management, Property Protection and Inspections and Auditing:

- **Personal Identity and Logistics information**
  - Employee First Name and Last Name
  - Employee Email
  - Employee Agency
  - Employee Office Address
  - Employee Telephone Number

- **General Facility Information**
  - Facility ownership type
  - Any co-located Agencies
  - Facility size & number of employees
  - Surrounding Environment
  - Police/Fire department jurisdiction & response time
  - HSPD-12 credential & AGAR Advisory 81 compliance (i.e. identity proofing, criminal history check)
  - Procedures for employee work in remote locations

- **Threat History**
  - 2 year & 2 mile radius crime/threat history
  - Physical Damage from Natural Disasters (earthquake, flood, hurricane, wild fire)

- **Asset classification**
  - Key structures & buildings
  - Legal & financial file storage (i.e. Farm contracts, deeds, checks, tax forms)
  - Mission critical & high value assets (i.e. the presence of PII, office/IT equip, communication devices, fleet vehicles)
  - Any poisonous, hazardous, or flammable material storage
- **Access Control Management**
  - Facility & asset access control system/management

PIV-A data elements include Personal Identity and Logistics information:

- Cardholder Unique Identifier (CHUID)
- Person Globally Unique Identifier (PGUID)
- User Principal Name (UPN)
- Person Identifier (PID)
- Agency
- Service Start Date
- Card Status

- Employee First Name, Middle Name, Last Name, E-mail
- Date of Birth
- Employee Type
- Employee Status
-
- Employee Photo
- Employee Work Location
- FBI Check

1.2 What are the sources of the information in the system?

The ePACS Applications Toolkit employs three uses for information within the system as described below.

1. Credentialing, Identity Verification, and Access Management - The ePACS and PIV-A Applications primarily use the information collected for these purposes. Information collected will allow individuals to obtain credentials needed for logical and physical access to USDA and its information systems.

2. Risk Assessment - GeoSIS and CRIS use information collected from local, state, and federal agencies to determine the risks associated with critical USDA infrastructures in the event of disaster.

3. Decision Support - GeoSIS and CRIS use the information to provide management site security information to maintain Continuity of Operations (COOP) and Continuity of Government (COG).

1.3 Why is the information being collected, used, disseminated, or maintained?

Each application within the ePACS Application Toolkit are focused on supporting the USDA efforts to comply with HSPD-12 Regulations while meeting the requirements outlined in FIPS 201-1 and OMB M-11-11.

- ePACS (Lenel) – To interface with the local physical access control systems (PACS), providing the required authoritative identity data from the government developed identity management system.

- GeoSIS - Provide an assessment of risk to the organization for operation and management purposes. These assessments allow the organization to enhance its response to potential threats. Information is gathered from local, state, and federal agencies to support OHSEC's Continuity of Operations (COOP), and Continuity of Government (COG) initiatives.

- CRIS - To identify facility assets, vulnerabilities, and threats in order to analyze and manage potential risks. CRIS satisfies numerous physical security requirements, including Interagency Security Committee (ISC) Assessment frequency, ISC Facility Security Level (FSL) determination Homeland Security Presidential Directive-12 (HSPD-12) for PIV.

- PIV-A - Act as a card issuance system which will integrate with the existing USDA OCIO EEMS Infrastructure. The system will provide a process allowing individuals to manage the lifecycle of their credentials for LACS and PACS to USDA information systems and buildings.

1.4 How is the information collected?

Information is collected in several ways within the ePACS Applications Toolkit. The designated data fields populated into ePACS is collected via a designated interface with the OCIO EIMS. Information for CRIS and GeoSIS is gathered through surveys and interviews with facility managers. Public information is also collected for site security assessments produced by GeoSIS.

1.5 How will the information be checked for accuracy?

Within ePACS and PIV-A, automated referential integrity checks and business rules are performed on the data before it is disseminated from the OCIO authoritative sources to the respective applications. These are conducted in a staging database before being transferred into the ePACS Applications Toolkit. Data integrity reviews based on a 95% confidence interval on the entire ePACS Application Toolkit record population will be performed on a recurring basis.

GeoSIS and CRIS facility assessment data is collected based on previously aggregated data developed by local, state and federal agencies. Facility assessment data will be performed by OHSEC (or Agency) Security Analyst, who develops the risk mitigation recommendations.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The ePACS Applications Toolkit is part of the Identify and Access Management Investment incorporating all USDA HSPD-12 systems. The HSPD-12 mandates all Federal departments to protect the identity and access to both physical and logical assets. Based upon this directive, National Institute of Standards and Technology (NIST) developed FIPS 201-1, which includes a description of the minimum requirements for a Federal PIV system.

Formal Interagency Security Agreements (ISAs) have been established between the OCIO and OHSEC regarding the interface between EEMS/EIMS and the ePACS Applications Toolkit.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The primary data element identified as PII within the ePACS Application Toolkit is photographs. Therefore, there are minimal privacy risks associated with the collection and sharing of information within the ePACS Applications Toolkit. Most of the information collected is for credentialing purposes and comes from sources approved by USDA.

In addition, the ePACS Applications Toolkit is in Phase I of the USDA Certification & Accreditation (C&A) process. Upon receipt of an Authority to Operate (ATO), the ePACS Applications Toolkit will have successfully completed Phase II and additional testing to ensure technical safeguards are well defined and applied to maintain compliance with NIST 800-53 Rev. 3 controls.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

Each application within the ePACS Application Toolkit are focused on supporting the USDA efforts to comply with HSPD-12 Regulations while meeting the requirements outlined in FIPS 201-1 and OMB M-11-11.

- ePACS (Lenel) - To interface with the local physical access control systems (PACS), providing the required authoritative identity data from the government developed identity management system.

- GeoSIS - Provide an assessment of risk to the organization for operation and management purposes. These assessments allow the organization to enhance its response to potential threats. Information is gathered from local, state, and federal agencies to support OHSEC's COOP and COG initiatives.

- CRIS - To identify facility assets, vulnerabilities and threats in order to analyze and manage potential risks. CRIS satisfies numerous physical security requirements, including ISC Assessment frequency, ISC FSL determination HSPD-12 for PIV.

- PIV-A - Act as a card issuance system which will integrate with the existing USDA OCIO EEMS Infrastructure. The system will provide a process allowing individuals to manage the lifecycle of their credentials for LACS and PACS to USDA information systems and buildings.

2.2 What types of tools are used to analyze data and what type of data may be produced?

ePACS - Lenel OnGuard only correlates limited information related to cardholders and is stored within the database. Data produced includes site badge credentials and database archival reports.

PIV-A - system produces identification credentials according to requirements outlined for HSPD-12 compliance.

GeoSIS - Data collaboration is provided by Microsoft SharePoint. A COTS product, ArcGIS (Environmental System Resource Institute ESRI), provides an integrated collection of GIS software products to meet all spatial analysis.

CRIS - Information is collected via surveys sent via SSL encryption or through an HTTPS protected web-based portal.

PIV-A - Uses multiple components to process data for credentialing. MyID is a web application for card activities. Also in place is Microsoft Certifying Authority for issuing trusted certificates.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

The ePACS Applications Toolkit has two applications (GeoSIS and CRIS) that provide an assessment of risk to the organization for operation and management purposes. These assessments allow the organization to enhance its response to potential threats. Information is gathered from local, state, and federal agencies. Below is a description for each application.

- CRIS - This application collects criminal history for individual facilities from State and Local law enforcement agencies to determine the threat level. These threats include terrorist attacks, natural hazards, unintentional hazards and common crimes.

- GeoSIS - This application collects data to provide site specific assessments based on data collected from facilities and geographic surroundings of USDA critical infrastructures. The chart below shows the external sources of information and their uses.

External Source	Source Description

External Source	Source Description
FSA NAIP Imagery	1 Meter Aerial Imagery
Forest Service Fire Hazard Mapping	Current and historical smoke and fire detection by NASA MODIS Satellite.
NOAA Live Weather Feed	Provides a radar mosaic for weather accumulation
NHSS-USGS Hazards	Hurricanes
NHSS-USGS Hazards	Wildfires & Perimeters
NHSS-USGS USDATA	Federal Lands
ESRI Base Maps	Street, Satellite, Shaded Relief, Topography, Physical
FEMA Flood Hazard Mapping	Provides flood hazard areas and historical flood data

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

There are minimal security risks associated with the collection and sharing of information within the ePACS Applications Toolkit. Most of the information collected is for credentialing purposes and comes from sources approved by USDA. External Sources of information are gathered through external resources and imported into the ePACS Applications Toolkit. Firewall rules have been established in conjunction with NITC to ensure that the systems import and export only valid file types (.csv, .kmx, .jpg). In addition, the ePACS Applications Toolkit is in Phase I of the USDA Certification & Accreditation process. Upon receipt of an Authority to Operate, the ePACS Applications Toolkit would have successfully completed Phase II and additional testing to ensure technical safeguards are well defined and applied to maintain compliance with NIST 800-53 Rev. 3 controls.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

Information within the ePACS Application Toolkit will be retained for six months and then deleted six months following that date.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

The retention period schedule that the ePACS Application Toolkit follows is in accordance with NARA standards.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

ePACS Applications Toolkit archival data is sometimes requested by employees at USDA agencies. Any data requests must be processed through the DM Freedom of Information Act (FOIA) Officer to the system owner.

Section 4.0 Internal Sharing and Disclosure

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Under the USAccess Shared Services Program, GSA provides EIMS authoritative data from USDA's human resources systems (EmpowHR, Personnel Payroll, and Non-Employee Identification System [NEIS]), which provides regular data transfers to ePACS and PIV-A. This information is classified as Security Management and Personal Identity and Logistics Information.

GeoSIS collects facility related information from other USDA information management systems, such as Corporate Property Automated Information System (CPAIS). In addition, there are plans to have CRIS facility assessments imported into GeoSIS. This information is classified as follows: Logistics Management, Public Resources, Facility and Infrastructure Management, Inspections and Auditing.

CRIS use interviews and surveys to collect information from each USDA facility through a locally assigned Security Analyst. This information is classified as Logistics Management, Public Resources, Facility and Infrastructure Management, Inspections, Property Protection and Auditing.

4.2 How is the information transmitted or disclosed?

Each Application within the ePACS Application Toolkit has various secure methods for transmitting data. Generally, the disclosure of information is prohibited based on the "Need-to-Know" principle as those with authorized interest will have been granted access. To collect data from the USDA authorized information systems please note the following:

ePACS (Lenel) - ePACS takes the information provided through the EIMS interface and processes it through a Master Security Database (MSD), which prepares it for placement in the Master PACS Database (MPD) and final distribution to secure agency access control segments within three PACS Regional Databases (PRD). The information is transferred via secure IPSEC methods.

GeoSIS - There are security concerns related to connecting directly to highly secure enterprise databases, therefore a controlled subset of a database dump or a confined query will be carried out to pull only necessary pieces of information from such systems.

CRIS - Facility assessment templates are developed by authorized on-site security analysts. Facility assessments are completed via a web-based assessment tool.

PIV-A - The MyID Web Application will operate as a role based portal hosting the user operations provided by the system. The MyID Web application will runs as a .Net application communicating over a DCOM interface to the MyID server components. This interface will have the ability to integrate with a standard LDAP v3 directory such as Microsoft's Active Directory.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Information is permitted to be collected only from Department authorized information systems. Each user is required to agree to the Rules of Behavior which deny the sharing of information. However, if additional sharing or collection is required and approved, users would have to submit a request per the guidelines defined in the ePACS Configuration Management Plan.

Communications will be protected by mechanisms defined in NIST 800-53 Rev. 3 by NITC in the PaaS environment. These controls will ensure that all data is coming from servers are encrypted. Also, data in transit within the ePACS Lenel component will be FIPS 140-2 compliant as Lenel is an authorized vendor of FIPS compliant equipment according to NIST requirements.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Information within the ePACS Application Toolkit is not shared with external organizations. However, if external access is required and approved, users would have to comply with the USDA Two Factor Authentication. This includes having applicable eAuthentication Service Credentials, RSA Token and/or a Computer Network Account provided by OCIO.

5.2 Is the sharing of Personally Identifiable Information (PII) outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the PII outside of USDA.

PII is not permitted to be shared outside of the Department. Each user is required to agree to the Rules of Behavior which deny the sharing of information. In addition, CRIS Facility Assessments are also denied public sharing under the exemptions of the Freedom of Information Act (FOIA). The statement attached to reports is as follows:

"Controlled Unclassified Information (CUI) Attachment - Disseminate on Need-to-Know Basis Only

This document contains information which may be exempt from mandatory disclosure under FOIA. Exemptions 2, 7a, and 7f of the Act apply, 5 U.S.C. §552(b)."

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Information is not permitted to be shared outside the Department. Each user is required to agree to the Rules of Behavior which deny the sharing of information.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Information is not permitted to be shared outside the Department. Each user is required to agree to the Rules of Behavior which deny the sharing of information. However, if external access is required and approved, users would have to comply with the USDA Two Factor Authentication. This includes having applicable eAuthentication Service Credentials, RSA Token and/or a Computer Network Account provided by OCIO.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

All users, owners, and administrators of the ePACS Applications Toolkit will be required to acknowledge and agree to the Rules of Behavior of each application within the system. In addition, all users, and owners will be required to undergo training for the use and potential dissemination of information contained in various modules as applicable.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

During the registration process users are provided an opportunity to decline providing information. However, failure to provide information will deny the user access to the system. Most of the information collected in the ePACS Application Toolkit is for the credentialing process to gain access to USDA and its information systems. Without compliance, users can not be processed for authorization or sponsored for credentials. This applies to LincPass, PIV-A and eAuth Level 2 credentials.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Information collected from individuals will primarily be used for the credentialing process, therefore providing the information individuals consent to be processed for access to USDA and use of its information systems. Individuals will be processed for either a LincPass or PIV-A credential.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Individuals are notified about the processing of their information during the registration process. Prior to access being granted for use of applications within the ePACS Application Toolkit, system users will be required to acknowledge and agree to the Rules of Behavior of each application within the system. These measures have been implemented to prevent individuals from being unaware of the collection and processing of information. Failure to agree to these measures will explicitly deny the individual access to USDA and its information systems. This applies to both employees and non-employees seeking to gain access to the ePACS Applications Toolkit.

Section 7.0 Access, Redress and Correction

7.1 What are the procedures that allow individuals to gain access to their information?

Following the registration process, access to privacy information is limited to individuals within the system. However, using the PIV-A system, users can access a PIV-A terminal or have the software installed on their USDA system to manage the lifecycle of their credentials. This includes updating a PIN, or requesting replacement cards.

The facility information collected by GeoSIS is publicly available and access to the ePACS Applications Toolkit is not required.

The facility information collected by CRIS is not publicly available and access to the ePACS Applications Toolkit is not required. The CRIS Security Reports contain the following statement to restrict access:

> *Controlled Unclassified Information (CUI) Attachment - Disseminate on Need-to-Know Basis Only*
>
> *This document contains information which may be exempt from mandatory disclosure under FOIA. Exemptions 2, 7a and 7f of the Act apply, 5 U.S.C. § 552(b).*

7.2 What are the procedures for correcting inaccurate or erroneous information?

Within ePACS and PIV-A, automated referential integrity checks and business rules will be performed on the data before it is collected from the other sources. Additional referential integrity checks and business rules will be performed on the data in a staging server before being transferred into the ePACS Applications Toolkit. Data integrity reviews based on a 95% confidence interval on the entire ePACS Application Toolkit record population will be performed on a recurring basis.

GeoSIS and CRIS facility assessments data is collected based on previously aggregated data developed by local, state, and federal agencies. Facility assessment data will be OHSEC (or Agency) Security Analyst, who develops the risk mitigation recommendations.

7.3 How are individuals notified of the procedures for correcting their information?

During the registration process users are provided instructions for managing their credentials. This includes accessing the PIV-A or Card Confirmation Server (CCS) to manage the properties of their credentials. Facility reports within GeoSIS and CRIS are readily available for users on the web portal for each application. Also, individuals are provided training on using the various applications.

7.4 If no formal redress is provided, what alternatives are available to the individual?

A contact list including information for customer support is provided to each individual during registration.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

The only privacy risk associated with redress available to individuals is the availability of the system during a major disruption. The ePACS Applications Toolkit Disaster Recovery Plan provides details on recovering each application during system outage. A Disaster Recovery System is in place which will allow individuals to maintain logical and physical access to USDA facilities and information systems.

Section 8.0 Technical Access and Security

8.1 What procedures are in place to determine which users may access the system and are they documented?

Each application within the ePACS Applications Toolkit is role based and privileges are based on the "Need-to-Know" principle. Registration and Approval of access to applications within the ePACS Applications Toolkit are documented in the ePACS Applications Toolkit Configuration Management Plan. Each application has three tiers of access that must be satisfied in order to receive access to the system. The first tier is meeting the two factor authentication guidelines of USDA. This includes a background investigation being processed to receive a credential and having received system access from the OCIO. The second tier is submitting a request for access and having a designated authority sponsor the individual. The final tier is being approved by the CCB and being authorized by the Director of OHSEC.

8.2 Will Department contractors have access to the system?

Yes. Access to the ePACS Applications Toolkit will be granted for both USDA employees and non-employees.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Prior to be granted access to the ePACS Applications Toolkit all individuals must acknowledge and agree to the terms of a Rules of Behavior document. Following this acknowledgement and based on the system access granted, training will be provided on the application of the tools, as well as the protection of the information. In addition, all individuals supporting the mission of USDA with access to its computing systems must annually complete the Information Security Refresher provided by the OCIO.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The ePACS Applications Toolkit is currently in operations and maintains an Authority to Operate (ATO) expiring in October 2011. It is currently undergoing an updated Phase I of the Certification & Accreditation process.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The ePACS Applications Toolkit has been categorized as a moderate system per FIPS 199 Security Categorization. To protect the data within the ePACS Applications Toolkit, the Recommended Security Controls for Federal Information Systems and Organizations developed by NIST will be applied. These controls are defined in the Special Publication 800-53 Revision 3.

Within NIST SP 800-53 Rev. 3, are 18 families of controls that include, but are not limited to, Access, Auditing, Identification, Authentication and Media Protection. Compliance with these controls will be a Hybrid effort supported by OHSEC, the system maintainer (CRI) and hosted by NITC in a PaaS environment. The system maintainer will be responsible for ensuring compliance from the application and database perspective, while NITC, as the host, will provide oversight of the Operating System, Hardware, Network and Physical Access to the Data Center where the ePACS Applications Toolkit virtual environment is located. Additional details regarding the compliance with the controls designed to protect data within the ePACS Applications Toolkit will be documented in the ePACS Applications Toolkit System Security Plan (SSP). Concepts for each family of controls are described below.

Access - OHSEC maintains the access control policies and procedures of the ePACS Applications Toolkit adhering to the USDA Departmental Regulation (DR 3505-003). Access to the applications is based on the "Need-to-Know" principle. All users are granted access by meeting the requirements of the USDA two factor authentication process, receiving an e-Authentication Service Level 2 account, and being sponsored by a designated authority for application level access which must be approved by the Director of OHSEC. On a monthly and annual basis, the ePACS Project Management Office (PMO) conducts account access reviews to determine if access is still granted. Accounts that are inactive for a period of 60 days or more should be terminated. Each system maintains separation of duties and least privilege based on roles. The various roles within the ePACS Applications Toolkit are System Administrator, Security Officer, Security Analyst, Visitor, and Operator.

Auditing - OHSEC maintains a daily, weekly and monthly auditing schedule and all data is stored in increments using back-up tapes which are maintained by the USDA provider, Iron Mountain. This information is stored for six months in accordance with the retention schedule put in place by NARA. NITC, as the PaaS provider, maintains a daily audit of access to the system to ensure malicious attempts to obtain information are not successful. In addition, a monthly security report is developed by the ePACS Applications Toolkit and provided to the officials within OHSEC.

Identification and Authentication - All individuals granted access to the system must undergo a Background Investigation (BI). Once the BI has been completed, a request for access is processed, which must be submitted by a designated authority and approved by the CCB and Director of OHSEC in accordance with guidelines defined in the ePACS Applications Toolkit Configuration Management Plan.

Media Protection - All servers supporting the ePACS Applications Toolkit are physically protected by measures in place by NITC. In addition, all servers have FIPS encryption enabled. Within the ePACS (Lenel) system, all data in transit is FIPS 140-2 enabled as Lenel is an authorized FIPS provider as confirmed by NIST.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

There are minimal security risks associated with the collection and sharing of information within the ePACS Applications Toolkit. Most of the information collected is for credentialing purposes and comes from sources approved by USDA. In addition the ePACS Applications Toolkit is in Phase I of the USDA Certification & Accreditation process. Upon receipt of an ATO, the ePACS Applications Toolkit will have successfully completed Phase II and additional testing to ensure technical safeguards are well defined and applied to maintain compliance with NIST 800-53 Rev. 3 controls.

Section 9.0 Technology

9.1 What type of project is the program or system?

The ePACS Application Toolkit is a Major Application operating under a Moderate Security Categorization per FIPS 199. The ePACS Application Toolkit is comprised of four sub-systems all supporting the USDA efforts to comply with HSPD-12 regulations while meeting requirements defined by FIPS 201-1 and PIV Compliance. The four sub-systems are as follows:

- ePACS (Lenel)
- GeoSIS
- CRIS
- PIV-A

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

All privacy concerns are mitigated by three factors, which are all required by USDA guidelines per NIST Recommendations. The first factor is that individuals must meet the

requirements of the USDA two factor authentication process. This includes having a LincPass or eAuthentication Service account and RSA Token provided by OCIO. Secondly, all individuals who access the ePACS Applications Toolkit must request access via a USDA Designated Authority. Access is granted following approval by the CCB and authorization being granted indirectly by the Director of OHSEC. Thirdly, following the approval of credentials, but before being granted access, all individuals who obtain access to the ePACS Applications Toolkit must acknowledge and agree to the terms of the Rules of Behavior.

On another note, there is one function within the ePACS Application Toolkit that may raise security concerns and that is the secure web-based external interface of the PIV-A. This web server will provide a service needed for external Web access. The service will be a distribution point for the Certification Revocation List (CRL). The Certifying Authorities CRL will be published to the Web server so that is publicly available to external systems without exposing the CA. The CRL is a public list and does not contain any information that would compromise the use of the system. As a result it will be published in an unprotected space where it is readily available over the internet.

Responsible Officials

Name:	**Richard Holman**
Title:	**Chief, Physical Security Division**
Office:	**Departmental Management DM, Office of Homeland Security and Emergency Coordination (OHSEC)**
Address:	**Reporters Building** **300 7th Street SW, Suite 0034** **Washington DC, 20024**
Phone:	**202-720-3901**
Email:	**Richard.Holman@usda.gov**

Name:	**Mike Defrancisco**
Title:	**Deputy Chief, Physical Security Division**
Office:	**Departmental Management DM, Office of Homeland Security and Emergency Coordination (OHSEC)**
Address:	**Reporters Building** **300 7th Street SW, Suite 101** **Washington DC, 20024**
Phone:	**202-401-0665**
Email:	**Mike.Defrancisco@usda.gov**

Name:	**Mike Schaum**
Title:	**Security Specialist, Physical Security Division**
Office:	**Departmental Management DM, Office of Homeland Security and Emergency Coordination (OHSEC)**
Address:	**Reporters Building** **300 7th Street SW, Suite 101** **Washington DC, 20024**
Phone:	**202-401-0662**
Email:	**Mike.Schaum@usda.gov**

Name:	**Carl Holmes**
Title:	**Information System Security Program Manager**
Office:	**Departmental Management, Office of Chief Information Officer**
Address:	**USDA South Building** **1400 Independence Avenue, Suite 1456** **Washington DC, 20250**
Email:	**carl.holmes@dm.usda.gov**

Approval Signature

Position of Signatory	*Name of Signatory*	*Date Signed*	*Signature*
Approving Authority	Mike McGuire	6-2-11	
Certifying Authority	Christopher Wood	5-11-2011	
System Owner	Richard Holman	22 Apr 2011	
User Representative	Mike DeFrancisco	4-26-11	
OHSEC-ISSO	Mike Schaum	4-26-11	for
Project Manager	Frank Bowen	4-26-11	
ISSPM	Carl Holmes	5-26-11	
DM-ISSO	John Brown	4-26-11	