Automated Safety Incident Surveillance Tracking System (ASISTS) V. 2.0

Graphical User Interface (GUI)

Security Guide

"SENSITIVE INFORMATION"

June 2002

(Revised September 2008)

Department of Veterans Affairs
Office of Enterprise Development
Management & Financial Systems

Revision History

Initiated on 09/02/08

Date	Description (Patch # if applicable)	Project Manager	Technical Writer
09/02/08	Enhancements from Patch OOPS*2*15 – Privacy Act issues, modifications to the CA-7 to meet Department of Labor changes to the form	Zach Fain	Corinne Bailey

Preface

Purpose of the Security Guide
The Security Guide specifies parameters controlling the release of sensitive information related to the Automated Safety Incident Surveillance Tracking System (ASISTS) V. 2.0 software.

This document will be excluded from any Freedom of Information Act (FOIA) request releases. Distribution of this document is restricted to the Information Resource Management (IRM) Service and ADP Security Officer (ADPSO). Since certain keys and authorizations must be delegated for proper management of the system, information about these items may be found elsewhere in the technical and user manuals.

Reference Numbering System
This document uses a numbering system to organize its topics into sections and show the reader how these topics relate to each other. For example, section 1.3 means this is the main topic for the third section of Chapter 1. If there were two subsections to this topic, they would be numbered 1.3.1 and 1.3.2. A section numbered 2.3.5.4.7 would be the seventh subsection of the fourth subsection of the fifth subsection of the third topic of Chapter 2. This numbering system tool allows the reader to more easily follow the logic of sections that contain several subsections.

Table of Contents

1 Introduction

1.1 Overview

ASISTS (Automated Safety Incident Surveillance Tracking System) V. 2.0 implements the inclusion of a graphical user interface (GUI) on the original roll and scroll version of ASISTS. One of the few enhancements included in ASISTS GUI was the inclusion of a multifaceted report for reporting on data from the incident report. The information provided in this guide is directed at the server side requirements (M and FileMan) for this package.

1.2 Security Management - Restrictions for Using Fiscal and Procurement Data

The ASISTS V. 2.0 package manages the collection of information relating to accidents and completion of workers' compensation claims for employees at your facility. The need for package security is addressed throughout this software, affording every effort to restrict the mishandling of ASISTS functionality.

1.3 Modifying Routines

The modification of ASISTS V. 2.0 routines is covered by the Veterans Health Administration (VHA) Manual, M-11, "Information Resources Management", Chapter 9, "Software Management". The complete text may be found at http://vista.med.va.gov/policies/m-11ch9.doc. A portion is quoted below:

9.11 PROCEDURES FOR SITE IMPLEMENTATION

b. **Local Modification of Software**

(1) Where a national package implements a controlled procedure (e.g., payroll processing, procurement, fee basis, medical quality control) which in turn reports data to a data base outside the VHA environment (e.g., CALM, Automated Medical Information System (AMIS)), there must be no alteration of that package except by the Development ISC. National package routines relating to security features or fiscal integrity also must not be altered except by the Development ISC.

…

(5) Local modifications of national package routines are strongly discouraged. If local modifications are made to existing routines in national packages it will then be the responsibility of the modifying health care facility to maintain those modifications.

1.4 Modifying Data Dictionaries

The modification of ASISTS V. 2.0 data dictionaries is covered by the Veterans Health Administration (VHA) Manual, M-11, "Information Resources Management," Chapter 4, "Data Base Administration." The complete text may be found at http://vista.med.va.gov/policies/m-11ch4.doc. A portion is quoted below:

4.07 PROCEDURES FOR MODIFICATIONS TO DATA DICTIONARIES

a. Modifications to national package data dictionaries should be restricted to the addition of new data elements and to the creation of input and output templates to meet specific needs of local sites. To ensure the capability of installing new releases of the application packages, it is important that any local additions to the data base be made in areas that will not conflict with elements contained in the nationally distributed data base.

b. When adding new data elements to the VA FileMan data dictionary, the numbering conventions used for creating new files should also be used for data elements.

(1) A data element number should be entered that is in the numbering range of the assigned numbering prefix multiplied by 1000.

(2) The same convention should be applied to global subscripts for local data add-ons to previously defined globals.

c. The VA FileMan subdictionary numbers should be assigned at the high end of the numbering sequence, following the numbering convention outlined. For example, a VA FileMan subdictionary number added to the Patient file (File 2) by station 368 should be 2.368001, a second subdictionary should be assigned 2.368002, and so forth.

d. The VA FileMan data dictionary may be modified only through tools provided by the VA FileMan or by tools specifically referenced in the VA FileMan Programmer's Manual.

e. To keep conflicts with cross-references to a minimum, field facilities creating custom cross-references must use the number range assigned to the site and prefix with "AZ" or "Z".

(1) National packages are not permitted to use these cross-references.

(2) Cross-reference numbers should be assigned based on the station number multiplied by 1000.

f. All other types of local data modifications to national packages are strongly discouraged. If local modifications are made to existing data elements in a national package data dictionary, it will then be the responsibility of the site to maintain those modifications as new versions of the package are installed.

```
g.  When software components are incorporated into the package, the names
associated with the new components (e.g., routines, options, templates)
should be prefixed by the package namespace followed by the letter "Z".

  (1)  For example, a local option called "LOG" for the PSIV package
  would have the option name "PSIVZLOG".

  (2)  Prefixing allows the site to readily differentiate between
  components developed locally and those associated with the DHCP
  national packages.

  (3)  Namespaces of one, two, three, or four characters followed by "Z*"
  shall not be exported in nationally developed software, but shall be
  reserved for local use.
```

In accordance with quoted section 4.07a. above, some dictionaries should never be altered as this data is used in the transmission of Workers' Compensation Claims to the Department of Labor (DOL). Alteration of these dictionaries may result in the rejection of and untimely submission of claims to DOL. These Dictionaries Are: ASISTS DOL Anatomical Location Codes file (#2261.1), ASISTS DOL District Office file (#2262.1), ASISTS DOL Type Of Injury Codes file (#2263), ASISTS DOL Source Of Injury Codes file (#2263.1), ASISTS DOL Cause Of Injury Codes file (#2263.2), ASISTS DOL Nature Of Injury Codes file (#2263.3), ASISTS DOL Provider Title file (#2263.5), ASISTS OWCP Chargeback Codes file (#2263.6).

1.5 Menu Assignments

The concern for package security includes the menus assigned to the ASISTS user. ***NO ASISTS USER should have access to all of the options available.*** The standardized menus that accompany this package were specifically designed to account for those functions that are performed by Supervisors, Employee Health, Safety Officers, Workers' Compensation Specialists, and Union Representatives.

2 Electronic Signature

2.1 Overview

A primary aspect of security in ASISTS involves the use of Electronic Signatures. All employees should have the ability to enter and edit their own Electronic Signature Code. This code is required for the employee, as well as their supervisor and the Safety Officer, Employee Health, or Workers Compensation specialist to electronically complete an incident report, CA1 or CA2 claim. Like the access and verify codes used when gaining access to the system, the Electronic Signature Code will not be visible on the terminal screen. These codes are also encrypted so that even when viewed in the user file by those with the highest levels of access, they are unreadable. Electronic Signature codes are required by ASISTS at every level that currently requires a signature on paper.

Those individuals with Electronic Signature Codes have a menu option, located on their secondary menu (User's Tool Box), that allows them to change their Signature Code at any time.

2.2 Electronic Signature Design

An Electronic Signature is designed as a two-part process and is described below.

> ***Identification*** (or "hashing") is system verification that the person who logged in is the same person accessing a document. This process of identification uses the Electronic Signature (ESIG) Code string, which it passes through a hashing algorithm and compares it to a string maintained in the user file of the person currently logged into the system. A match indicates (unless a user has "shared" his/her ESIG Code with another person) that the person entering the ESIG Code is the "logged-in" user. The identification process can and is used independently of the record authentication function.

> ***Authentication*** (or "encoding") marks an electronic record within VistA with the identification of the user. This process takes the internal record number of the record being secured (i.e., the Signature Block Name of the person signing the record and that person's internal record number in the NEW PERSON file # 200) and passes it through a second algorithm to create a string. "Decoding" of the string occurs as the reverse of the process just described. The matching of the user Signature Block Name and the outcome of the Decoding process validates that the Electronic Signature is "tamper free".

3 ASISTS Security Keys & Other Features

3.1 Description of Security Keys

This list of security keys is also found in the ASISTS V. 2.0 Technical Manual.

OOPS DOL XMIT DATA
DESCRIPTION: Enables the holder of this key to manually transmit claims to the Austin Automation Center (AAC). This functionality will only be exercised if the original transmission failed and the Mailman message could not be read by the AAC. It locks the following option:
Manual Transmission of DOL Data [OOPS DOL MANUAL XMIT DATA]

OOPS XMIT 2162 DATA
DESCRIPTION: This key is used to manually transmit incident data to the ASISTS National Database at the AAC. It locks the following options:
Manual Transmit of National Database Data [OOPS MANUAL DATA XMIT]

3.2 Mail Groups

A listing and descriptions of Mail Groups appear in the ASISTS V. 2.0 Technical Manual.

3.3 Bulletins

A listing and descriptions of Bulletins appear in the ASISTS V. 2.0 Technical Manual.

3.4 Archiving/Purging

Currently, ASISTS does not implement any archiving or purging processes.

3.5 Contingency Planning

Using services must develop a local contingency plan to be used in the event of product problems in a live environment. The facility contingency plan must identify the procedure for maintaining the functionality provided by ASISTS V. 2.0 in the event of system outage. Field station ISOs may obtain assistance from their Regional Information Security Officer (RISO).

3.6 Interfacing

Currently there are no interfaces to external equipment in ASISTS V. 2.0.

3.7 Remote Systems

The following entries describe the data transmitted from ASISTS V. 2.0 to remote system/facility databases.

Completed CA1 and CA2 Claims
Completed and approved CA1 and CA2 claims are electronically transmitted in Mailman e-mail messages from ASISTS systems to the Austin Automation Center (AAC) in Texas. The TCP/IP handles accuracy within the mail transmission. Upon receipt, the AAC processes the claim and either forwards the claim electronically to the Department of Labor (DOL) or sends back a message detailing why the claim was rejected. Once the claim is received and processed by DOL, an additional message is relayed back to the AAC who forwards it back to the sending mail system. The message from DOL will contain either a confirmation or rejection notice.

Incident Report data transmissions
Data collected on the Incident Report is electronically transmitted in Mailman email messages from ASISTS systems to the VSSC group at the Austin Automation Center in Texas. When an incident report is closed by the safety officer, pertinent data elements from the incident report are sent to the aforementioned group. The program office implemented this process to improve statistical reporting, the tracking of system-wide problems, to identify opportunities for focused education, and to support research into the area of occupational medicine.

4 File Protection and Security Access

4.1 File Protection

The ASISTS V. 2.0 package files contain data that is pertinent to the filing of workers' compensation claims by employees and is covered by the Privacy Act. Therefore, the files used by ASISTS generally carry a high level of file protection. The data dictionaries for ASISTS should **NOT** be altered. Screening logic has also been enabled on some ASISTS files to prevent access through VA FileMan.

4.2 Files and Security Access

File #	Name	DD	RD	WR	DEL	LAYGO	AUDIT
2260	ASISTS ACCIDENT REPORTING	@	@	@	@	@	@
2261	ASISTS CHARACTERIZATION OF INJURY	@		@	@	@	@
2261.1	ASISTS DOL ANATOMICAL LOCATION CODES	@		@	@	@	@
2261.2	ASISTS CRITICAL TRACKING ISSUES	@		@	@	@	@
2261.21	ASISTS INCIDENT WEATHER FACTOR	@		@	@	@	@
2261.22	ASISTS INCIDENT SOURCE	@		@	@	@	@
2261.24	ASISTS PREVENTION METHOD	@		@	@	@	@
2261.3	ASISTS PERSONAL PROTECTIVE EQUIPMENT	@		@	@	@	@
2261.4	ASISTS SETTING OF INJURY	@		@	@	@	@
2261.45	ASISTS LOCATION OF INJURY DETAIL	@				@	@
2261.5	ASISTS PURPOSE FOR USING SHARPS	@		@	@	@	@
2261.6	ASISTS OCCURRENCE OF SHARPS INJURY	@		@	@	@	@
2261.7	ASISTS DEVICE/EQUIPMENT	@		@	@	@	@
2261.8	ASISTS RESULTS	@		@	@	@	@
2261.9	ASISTS SAFETY CHARACTERISTICS						
2262	ASISTS SITE PARAMETER	@	@	@	@	@	@
2262.1	ASISTS DOL DISTRICT OFFICE	@	@	@	@	@	@
2262.2	ASISTS DEVICE SIZE						
2262.3	ASISTS NEEDLESTICK BRANDS						
2262.8	ASISTS REASON FOR DISPUTE CODES	@		@	@	@	@
2263	ASISTS DOL TYPE OF INJURY CODES	@		@	@	@	@
2263.1	ASISTS DOL SOURCE OF INJURY CODES	@		@	@	@	@
2263.2	ASISTS DOL CAUSE OF INJURY CODES	@		@	@	@	@
2263.3	ASISTS DOL NATURE OF INJURY CODES	@		@	@	@	@
2263.4	ASISTS DOL OCCUPATION CODES						
2263.5	ASISTS PROVIDER TITLE	@		@	@	@	@
2263.6	ASISTS OWCP CHARGEBACK CODES	@	@	@	@	@	@
2263.7	ASISTS UNION INFORMATION						
2263.8	ASISTS BODY PART GROUPING	@		@	@	@	@