e-ISuite

WHITE PAPER

Prepared By:

SabiOso, Inc.
189 S. State Street
Suite 250
Clearfield, UT 84015

Prepared For:

IBA Project

Revision: R006

Wednesday, January 25, 2008

e-ISuite Background

The Incident Based Automation Project Team is tasked by the National Wildfire Coordinating Group (NWCG), as part of Phase 3 of the Incident Based Automation (IBA) project, to develop a browser-enabled version of I-Suite called e-ISuite. Part of this task is to define and develop an application that coordinates, consolidates and processes data to be used by the incident and other personnel to support incident management at a local and an enterprise level.

What is I-Suite?

The I-Suite application is a portable, client/server application that can be used at any emergency incident to capture data and help manage resources and costs at remote incident locations. The application is organized into modules based on the Incident Command System (ICS). These modules interact with each other providing real-time visibility of actions being taken by the different ICS sections at the incident. The data captured within I-Suite includes:

- Check-In Data
- Plans Data
- Demobilization Data
- Time Data
- Cost Data
- Injury/Illness Data
- Supply Data

What is e-ISuite?

e-ISuite is the next generation version of I-Suite and when fully implemented will replace the current I-Suite Application. The e-ISuite system is a web browser (e.g. Internet Explorer) enabled I-Suite application for use at the Incident Command Post (ICP) and in agency offices to manage emergency incidents and planned events. The use of e-ISuite at the ICP will be very similar to the current I-Suite application. e-ISuite used in agency offices will bring most of the current I-Suite capabilities to a person connected to the agency network via a web browser. At that level, it can be used for activities such as initial attack (IA), Type 3, 4 and 5 incidents, ABCD Miscellaneous fires and generating invoices for casual hires supporting activities like training, dispatch, and cache work. e-ISuite software will not need to be installed on the user's computer. No software licenses are required to use e-ISuite. A web browser is all each user will need to run the application.

There are two areas of use for the e-ISuite system:

- e-ISuite Enterprise System
- e-ISuite Remote Incident Site

The e-ISuite Enterprise System will be hosted on the USFS Fire and Aviation Management National Enterprise Support System (NESS) General Support System (GSS) at the National Information Technology Center (NITC), Kansas City, MO and will support all incidents at an enterprise level.

The e-ISuite Remote Incident version will be hosted on a server at an incident site. When a connection to the Internet is available, data can be transferred to and from the e-ISuite Enterprise System. When a connection to the Internet is not available, data can be transferred to a portable media device, which can then be taken to a computer with an Internet connection and transferred to and downloaded from the e-ISuite Enterprise System.

Benefits of e-ISuite

Benefits of Using e-ISuite at the Remote Incident Site:

- Install and update software on one computer instead of 20 or 30 computers.
- Administrative rights will not be needed on the user computers.
- Data from other sources can be easily retrieved (e.g. ROSS, ICBS, IQCS, etc.)
- e-ISuite data can be provided to other applications (e.g. ROSS, ICBS, etc.)

Benefits of Using e-ISuite at an Agency Office:

- No need to install software to utilize e-ISuite capabilities.
- Use e-ISuite capabilities for a wider range of activities. (e.g. IA, ABCD Misc. fires, training, etc.)
- Easily create and manage IAPs, costs, invoices, etc. for local resources.

General Benefits of e-ISuite:

- Centralized incident data.
- Complete incident life cycle from IA to close out.
- Data will automatically be stored and backed up.
- Data from all incidents using e-ISuite is available for analysis.
- Historical data will be available for many years.
- Supports a variety of incident management configurations and transitions.
- Improves the electronic payment process.

Using the e-ISuite Remote Incident Site Version

An Internet connection is NOT required to use e-ISuite at the Remote Incident Site. Running e-ISuite at the Remote Incident Site will be very similar to the current I-Suite application, except that installation of software is only required on the server computer located at the ICP.

The server computer will require installation of all application files and software components needed to run e-ISuite. These files and components will be easily installed and configured from an installation program or will come pre-installed and then easily configured on the server computer.

All e-ISuite user computers will be connected to a locally established network, just as they are today. The user will enter the address of the local e-ISuite server into their web browser, enter a user name and password, and begin using e-ISuite. User names and passwords will be assigned and managed at the Remote Incident Site.

If an Internet connection is not available for the e-ISuite server at the incident site, data can be transferred to and from the e-ISuite Enterprise System via an encrypted import/export file on a computer with an Internet connection.

If and when an Internet connection is obtained at the incident, the e-ISuite server at the Remote Incident Site can be configured to transfer data to and from the e-ISuite Enterprise System.

Using the e-ISuite Enterprise Version

A person with an e-ISuite Enterprise System user name and password and an Internet connection can use the e-ISuite Enterprise version of the application from their office using their web browser. They will be able to use e-ISuite for activities such as initial attack (IA), Type 3, 4 and 5 incidents, ABCD Misc. fires and generating invoices for casual hires for activities like training, dispatch, and cache work. e-ISuite specific software will not need to be installed on the user's computer. The e-ISuite Enterprise System will automatically send and receive data from other applications (e.g. ROSS, ICBS, IQCS, etc.) on a regular basis. Data from these other applications will be available for use within the e-ISuite Enterprise System.

If a user has access to other enterprise applications (e.g. ROSS, ICBS, etc), that same user name and password may be used to access the e-ISuite Enterprise System using a single sign-in methodology.

Transitioning Between the Host Agency and Incident Site

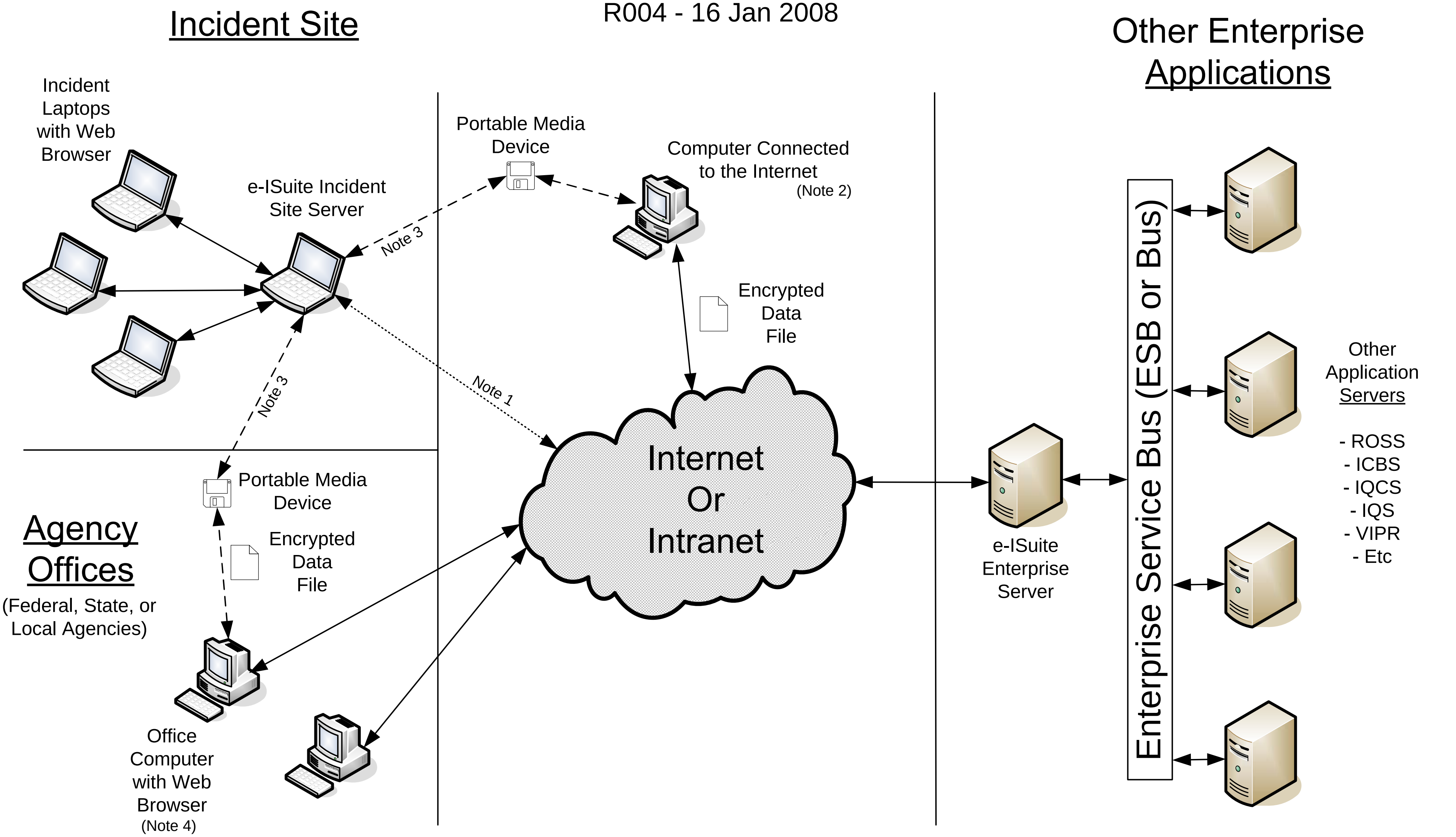
When an incident is being managed using the e-ISuite Enterprise System and management of the incident transitions to an Incident Management Team (IMT), e-ISuite data can easily be transferred to a remote e-ISuite server. As an incident winds down and management of the incident is transitioned to the host agency, e-ISuite data can easily be transferred to the e-ISuite Enterprise System and the incident can be managed from the agency office until completely closed out.

An incident does not have to be initially managed using the e-ISuite Enterprise System. An incident can be initially managed by an IMT using the e-ISuite Remote Incident Site version.

DRAFT

e-ISuite Conceptual Design

R004 - 16 Jan 2008



Incident Site

Incident Laptops with Web Browser

e-ISuite Incident Site Server

Note 3

Portable Media Device

Computer Connected to the Internet (Note 2)

Encrypted Data File

Note 1

Note 3

Portable Media Device

Encrypted Data File

Agency Offices

(Federal, State, or Local Agencies)

Office Computer with Web Browser (Note 4)

Internet Or Intranet

e-ISuite Enterprise Server

Enterprise Service Bus (ESB or Bus)

Other Enterprise Applications

Other Application Servers

- ROSS
- ICBS
- IQCS
- IQS
- VIPR
- Etc

NOTES:

1. A connection to the internet is not required to run e-ISuite at the incident site. Computers outside the incident site are not allowed to connect to the incident site server.
2. The computer connected to the internet could be located at the incident, agency office, library, etc.
3. The portable media device is hand carried to and from the incident site.
4. Computers at an agency office run e-ISuite directly from the e-ISuite enterprise server.
5. Established government standards for security, including fire walls and data encryption, will be implemented throughout the entire e-ISuite system.