Unit 1 – Introduction Instructor Notes

There are several ways to present the e-ISuite Introduction:

- *Instructor using the Intro PPT, students' attention on instructor, student computers closed.*
- *Students follow the Intro PPT on their computers while the instructor covers the materials.*
- *Instructor displays the webpage on the projector, students' attention on instructor.*

Instructor Curriculum and Helpful Resources are available at: https://www.wildfire.gov/application/eisuite

TOPICS COVERED IN THIS UNIT:

- Introduction
- Overview of the application
- Roles / Functionality

Introduction (Intro PowerPoint available on the website)

- Welcome
  ○ Introduce instructors ○ Trainees introduce themselves ○ Student sign-in sheet optional
- Logistics ○ Facilities – restrooms, drink and snack locations, emergency exits, other pertinent information ○ Student Certificates – Optional, this is not a pass/fail course.
  - ▪ Students are encouraged to learn as much as possible to efficiently use the application.
- Class Schedule ○ Start and stop times, lunch, and break times.

Overview

User Resources

Training materials and other helpful information are available for students in several formats and are accessible on the e-ISuite webpage. The materials have been developed to accommodate learning for new users and can also be used as a refresher for experienced users.

- Helpful Resources – This area provides access to documents containing supplemental information for users. This includes information on Site installation; network issues; Known Issues; IROC Imports; Financial Exports; and tips for writing custom reports. Additional information is added periodically.
- iNAP Accounts – The Integrated National Application Portal (iNAP) is accessed through their website: https://nap.nwcg.gov/NAP/. Click on the icon in the right upper corner, select Request User Account, and follow the instructions to request an iNAP account. iNAP Accounts are required to access e-ISuite Enterprise.
- User Guide – The User Guide is separated into functional areas to streamline information access and can be viewed online or printed individually. All the User Guide chapters can be printed if desired, and copies provided to the students.
- Quick Reference Cards (QRCs) – These "cards" provide streamlined information on various topics. QRCs are updated when changes to the application are implemented.

- Where to get HELP - The Helpdesk contact information is located on the Home Page of the e-ISuite webpage. Help is also available within the application by clicking on the HELP button at the top of the screen. This button provides a searchable tool accessible without leaving the application.

Differences between Enterprise and Site

See documentation for the roles of Account Manager and Data Steward for additional information on the differences in functionality between Enterprise and Site accorded those roles – this is where the major differences exist, along with accessing Enterprise and Site. The basic 'functional' areas are identical in Enterprise and Site.

 Enterprise ○ Web-based – stable internet access is required ○ No need to download an installation package – accessible by use of a URL ○ Can be used for any incident with stable internet connectivity ○ Incident Groups can be created to facilitate "Manage as Group" functionality ○ Housed at a central location – no back-ups needed ○ Users are required to have a valid iNAP Account with access to e-ISuite Production ○ Passwords are managed through the iNAP webpage ○ Users are added to an Incident User Access List in order to work in that incident – a user can be added to multiple incidents

○ All incidents should eventually be housed in Enterprise through a Data Transfer file from an incident managed using the Site version

 Site ○ Installation package downloaded and installed on computer

○ Accessed through a browser (e.g. Chrome, Edge) – no internet access is required ○ Can be used for all types of incidents ○ Can have up to 5 databases with multiple incidents in each database ○ Each incident in a database is part of the "Site Group", but can be managed individually or as a group –

"Manage as Group" functionality ○ User accounts are created for each database by an Account Manager, and have access to all incidents in that database - iNAP Accounts are not needed

○ iNAP Accounts do not allow access to Site; Site user accounts do not allow access to Enterprise ○ Database Management is required – including setting back-up intervals

○ Incidents can be started in Enterprise, transitioned to Site, and then transferred back to Enterprise;

or an incident can be started initially in Site and transferred to Enterprise at close-out

- Rules of Behavior:
  When logging into e-ISuite, a user must read and agree to the security statement that displays. All e-ISuite users must understand and follow the Rules of Behavior and the security principles and practices of their respective Agencies. All users are responsible for safeguarding the information collected, stored and maintained in the e-ISuite application. The system Rules of Behavior do not replace existing Agency policies, rather they are intended to enhance them.

- Security Principles:
  Users are to work within the confines of their authorized access or role. Users should not attempt to access functionality in the e-ISuite application to which they do not have authorization. Security violations include, but are not limited to:
  - ▪ Sharing of username and password pairs

- Sharing e-ISuite information or data with individuals who do not have an official need to know ▪ Violating other established security policies or procedures

If a user leaves their computer for any period, the application should be closed. At a minimum, their computer must be locked. This will ensure that no unauthorized person can access the e-ISuite application while the computer is untended. The e-ISuite application will automatically close after 2 hours of inactivity, per USDA security protocols.

An e-ISuite Site database should NOT be distributed to anyone except those outlined in other policies (e.g. to a transitioning IMT, jurisdictional unit, or authorized personnel). All Site databases are password-protected, and the password must meet the requirements as follows:

- Contain a minimum of 12 characters
- Contain at least 1 lowercase letter
- Contain at least 1 uppercase letter
- Contain at least 1 number
- Contain at least one of the following special characters: ! # % & * ^

- Personal Information (PII Data)
  PII Data is Personally Identifiable Information. e-ISuite no longer collects PII Data in the form of Social Security Numbers, Tax Identification Numbers (TIN), or personal addresses. The SSN has been replaced with the Employee Common Identifier (ECI) for AD employees; a contractor's TIN has been replaced by entering their UEI number; and personal addresses have been replaced with the address of the hiring agency. PII Data may still be entered (i.e. Date of Birth), but the collection of such data is discouraged.

  Because the presence of PII Data cannot be completely restricted, all data export files are encrypted for security purposes.

Roles and Functionality

Briefly describe the roles and functionality of each – more detail will be provided in the corresponding Unit in this curriculum. The User Roles PPT is helpful with this section, as well as the documentation on roles under Helpful Resources on the webpage.

Separation of duties requires privileged and non-privileged access. Privileged accounts only apply to the Site version. The user accounts have been designed to meet this requirement. Privileged user accounts in the Site version allow access to conduct database management activities, manage user accounts, assign roles, and manage the Message Board; non-privileged user accounts allow access to the corresponding functional area within the application.

Multiple roles can be assigned to user accounts; however, roles should be assigned according to the duties the user is expected to perform – the "least access" approach.

Some differences exist in the Account Manager and Data Steward roles in what each can perform in Enterprise and Site. *See below and the Roles ppt for the differences.*

Privileged User Roles and Functionality – Site Only

- Account Manager
- Create the initial Account Manager user account and database
- Manage the database, create additional databases
- Create other user accounts – both Privileged and Non-Privileged (A user account created in a Site database has access to all incidents in that database)
- Assign roles to the user accounts
- Reset user account passwords
- Enable / Disable a user account
- Disconnect a user account
- Post information on the Message Board

Non-Privileged User Roles and Functionality

- Account Manager **-** Enterprise
- Bring existing iNAP User Accounts into Enterprise
- Limited User Account management as Enterprise requires iNAP Accounts and they are created and managed in iNAP.
- Assign the Unit ID for the user
- Assign roles
- Enable / Disable a user account
- Disconnect a user account
- Remove an iNAP Account from Enterprise – this does not affect the account in iNAP
- Limited auditing at this time – can view who added/removed roles within a defined date range
  Password changes/resets and name changes must be performed on the iNAP website
- Data Steward
- Create/edit incidents
- Create/edit Incident Groups – Enterprise only
- Add non-standard Reference Data
- Add a user to an incident – Enterprise only
- IROC Import
- Financial Export
- Data Transfer
- Check-in Demob
- Add/edit/delete resources
- Change the status of a resource
- Roster/unroster resources
- Prepare resource documentation for demob
- Generate Plans reports
- Add/edit access to Common Data area
- IAP
- Create/edit an Incident Action Plan

- Use database information to create and fill in the ICS forms for the IAP
- Create/copy/delete forms and Plans
- Import PDF files to add to the IAP
- Export IAP files
- Time
- Add/edit/delete/roster resources
- Manage Employment Type of resources
- Post personnel, crew, and contract time
- Post adjustments
- Edit roster data
- Generate OF-288 and OF-286 invoices
- Generate other time reports
- Add/edit access to Common Data area
- Cost
- Add/edit/delete/roster resources
- Manage incident resources' costs
- View/edit daily cost records
- Create/manage Cost Groups
- Generate cost reports
- Access to Common Data
- Training Specialist
- Manage Trainee and Evaluator data
- Generate Trainee and Evaluator forms
- Generate other Training reports

Each functional area has specific reports associated with it that are available according to the role(s) assigned. These reports are covered in more detail in the functional area units of this course.

Custom Reports:

All non-privileged roles allow access to the Custom Reports area. Views and options available correspond to the role(s) assigned to the user. Custom Reports allow the following actions:

- Create and save non-standard reports Build queries that include:
    - General report characteristics
    - Column Builder ○ Sort Builder ○ SQL Viewer
- View report as PDF file
- Download data in Excel spreadsheet format
- Copy, Export and Import reports