



# **Classified Applications Process Overview**

Paul Halpin  
Electronic Data Systems  
Applications Product Line

# What is a Classified Seat?

- α A classified seat is a seat that is connected to SIPRNET IAW following DoD/DoN rules and regulations:
- PDS Guidebook (*Navy/Marine Corps IA Pub 5239.22*)
  - Department of the Navy (DON) Information Security Program (ISP) Regulation (*SECNAVINST 5510.36*)
  - DoD Information Technology Security Certification and Accreditation Process (DITSCAP) (*DODINST 5200.40*)
  - Navy Information Assurance (IA) Program (*OPNAVINST 5239.1B*)
  - Department of the Navy Physical Security (*OPNAVINST 5530.14C*)

## α **The process for rolling Classified seats is the same as Unclassified seats.**

- Classified seats bring their own set of rules, regulations, processes, policies, procedures, and deliverables that are significantly more complex than unclassified seats.

## α **There is no real policy for classified seats.**

- The aforementioned DoD/DoN documentation and policies all apply to NMCI classified seats. There is no one single document that coordinates and displays all existing DoD/DoN policies.

## α **NMCI is imposing new requirements on classified seats.**

- Under Navy direction, NMCI enforces existing policies and procedures across the Enterprise.
- There are no EDS policies to which the Navy is being required to adhere.

## α **Classified seats are all about SIPRNET, C&A and PDS.**

- While SIPRNET, C&A, and PDS are integral parts to the classified seat delivery process, they are not the “whole enchilada”.

- α All classified certifications must be complete prior to development of C&A package and IATO issuance.
  - Classified certifications are: OSS, CAA, CMS/EKMS, PDS (approval/disapproval), PDS POA&M (if required).
  
- α Certification & Accreditation is by definition “review and acceptance of the risk”, which is the final piece of the classified delivery process and cannot be completed until infrastructure is completed and valid certifications are provided.
  - Per Navy IA Pub 5239-13, C&A is the last event in the process prior to the system becoming operational. The C&A package is the bulk of the effort and is built as the process is in motion leading up to the critical path issue of review and risk acceptance by the DAA.

## α **Multiple process tasks can be run in parallel, not linearly.**

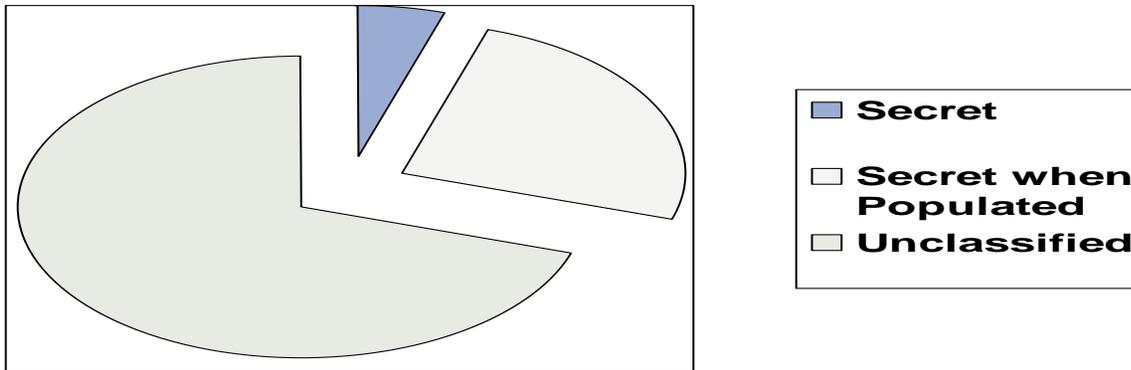
- Original process schedule laid out end-to-end required 15+ months going from survey to cutover; PDS construction timelines notwithstanding.
- EDS Classified Solution Product Management Team has compressed timeline down to 9 months; PDS construction timelines notwithstanding.

## α **Customer needs to be involved from the beginning.**

- Classified seat delivery is process intensive and working our way through this process requires integration and coordination between the Command and EDS.
- Key Naval Personnel
  - N6/Department Head or above
  - Physical Security Officer
  - Information System Security Manager (ISSM)
- Establish Echelon 2 ISSM oversight

# What Makes an Application Classified

- α **Legacy Applications with a Secret classification**
  - Smallest percentage of Classified Legacy Applications
- α **Unclassified or FOUO Legacy Applications that become classified Secret when populated with classified data**
  - A larger percentage of the Classified Legacy Applications
- α **Unclassified Legacy Applications running in a classified environment**
  - Most of the Classified Legacy Applications



- α **EDS processes and procedures for Legacy Application are the same for both the classified and unclassified testing.**
- α **The handling of material in the classified environment must follow the DoD security requirements.**
- α **The Classified environment is connected to the SIPRNET, all information, media, and data collected during this testing must be handled in a secure manner.**
- α **The Command Security Manager must be involved in the testing process and no information (data, information, or media) will be transmitted (either electronically, postal service, or other means) without the express approval of the Command Security Manager.**

# **Management of Classified Applications in ISF Tools**

- α **NETWARCOM approved the use of ISF Tools for the management of classified applications, providing the ‘sensitive data’, the Information Assurance (IA) data, was not entered. Associating the IA data to the classified application was a security concern and would cause ISF Tools to be considered a classified application.**
- α **To accommodate NETWARCOM’s ruling, the Application Deployment Solution (ADS) page used for entry of LADRA/IA/DAA data was modified such that if the IG-Increment selected was the ‘Classified’ Increment, the IA Update page for entering ports, protocols, boundaries, IP addresses, etc., is disabled. The Simple/Complex choice is selectable, but the IA data entry page normally presented for Complex applications is turned off for classified applications.**

## ☒ **Applications which can be entered into ISF Tools**

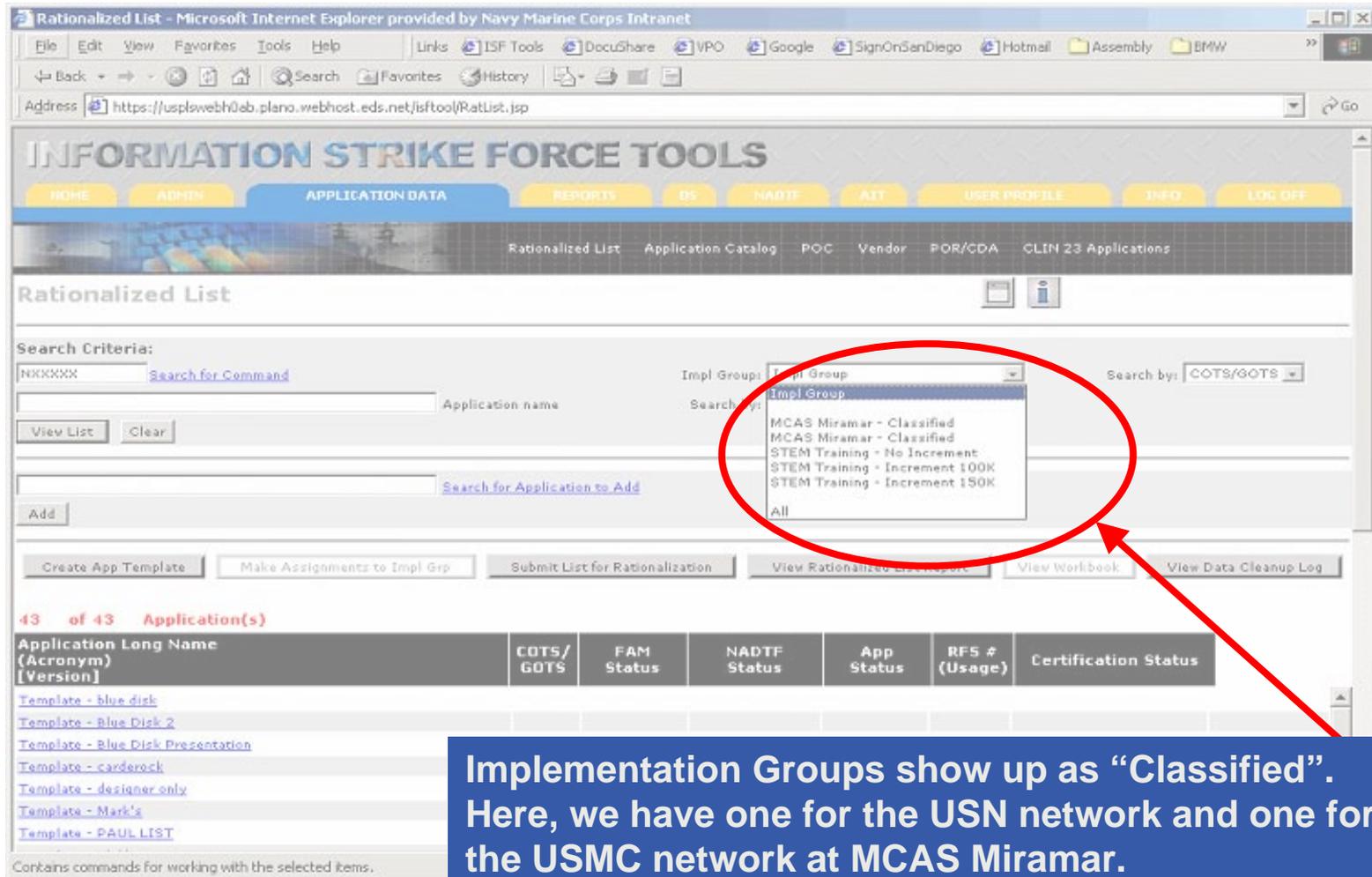
- Applications in which the name is not classified
- Unclassified or FOUO Legacy Applications that become classified when populated with classified data

## ☒ **Applications which cannot be entered into ISF Tools**

- Legacy Applications with a Secret classification
- Applications in which the name is considered classified
  
- These applications use manual submission and tracking methods.
  - Sites should download the Classified Legacy Application Rationalized List template (a Microsoft Excel Spreadsheet) from the NMCI website.

- **Classified applications will be entered into the same ISF Tools application as unclassified applications.**
- **Classified applications will be managed on the same Command/UIC Rationalized Lists as the Command's unclassified applications.**
- **The RFS for an unclassified application will be used for the same application running classified, and vice versa.**
- **The Information Assurance (IA) data entered during onsite LADRA testing and deployment activities is disallowed from being entered for classified applications.**

# View of Rationalized List Screen



**43 of 43 Application(s)**

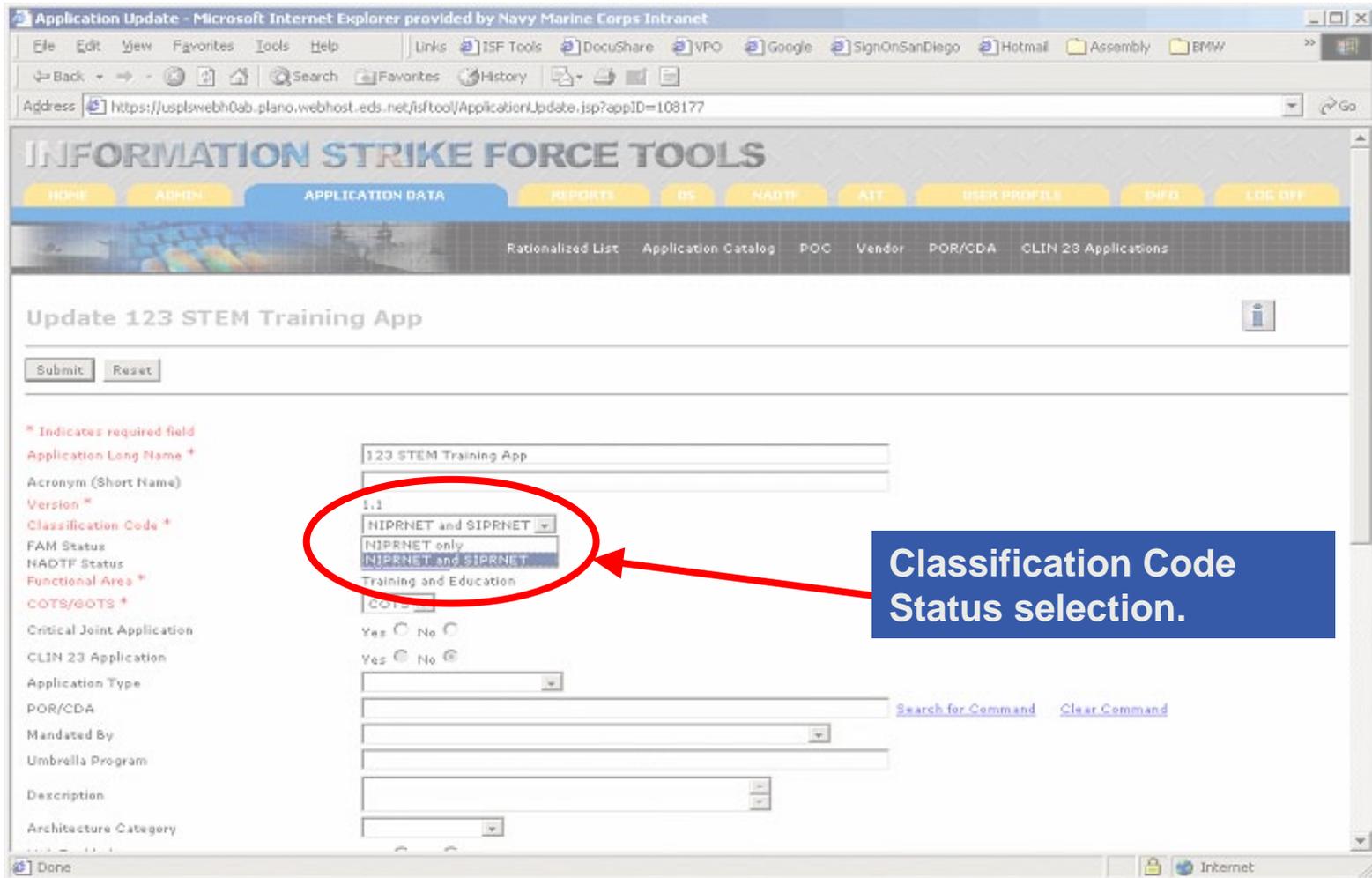
Application Long Name (Acronym) [Version]	COTS/GOTS	FAM Status	NADTF Status	App Status	RF5 # (Usage)	Certification Status
<a href="#">Template - blue disk</a>						
<a href="#">Template - Blue Disk 2</a>						
<a href="#">Template - Blue Disk Presentation</a>						
<a href="#">Template - carderock</a>						
<a href="#">Template - designer only</a>						
<a href="#">Template - Mark's</a>						
<a href="#">Template - PAUL LIST</a>						

Contains commands for working with the selected items.

Implementation Groups show up as "Classified". Here, we have one for the USN network and one for the USMC network at MCAS Miramar.

- α **All applications in ISF Tools have a ‘Classification Code’.**
  - NIPRNET only
  - SIPRNET only
  - NIPRNET and SIPRNET
- α **The Classification Code controls which Increment(s) of an IG the application can be assigned to.**
- α **The Classification Code is an application attribute. It will be the same value on all Rationalized Lists that include the application. It can only be set or changed via the Application Catalog page. If it is changed, all Rationalized Lists that include the application will reflect the change.**
- α **For startup purposes, all existing applications were set to ‘NIPRNET only’.**

# Classification Status on Application Record



Application Update - Microsoft Internet Explorer provided by Navy Marine Corps Intranet

Address: https://usplswebh0ab.plano.webhost.eds.net/isf/tool/ApplicationUpdate.jsp?appID=108177

## INFORMATION STRIKE FORCE TOOLS

HOME ADMIN APPLICATION DATA REPORTS DS NADTF ATT USER PROFILE INFO LOG OFF

Rationalized List Application Catalog POC Vendor POR/CDA CLIN 23 Applications

### Update 123 STEM Training App

Submit Reset

\* Indicates required field

Application Long Name \* 123 STEM Training App

Acronym (Short Name)

Version \* 1.1

Classification Code \*  
NIPRNET and SIPRNET  
NIPRNET only  
NIPRNET and SIPRNET

FAM Status

NADTF Status

Functional Area \* Training and Education

COTS/SOTS \* COTS

Critical Joint Application Yes  No

CLIN 23 Application Yes  No

Application Type

POR/CDA Search for Command Clear Command

Mandated By

Umbrella Program

Description

Architecture Category

Done Internet

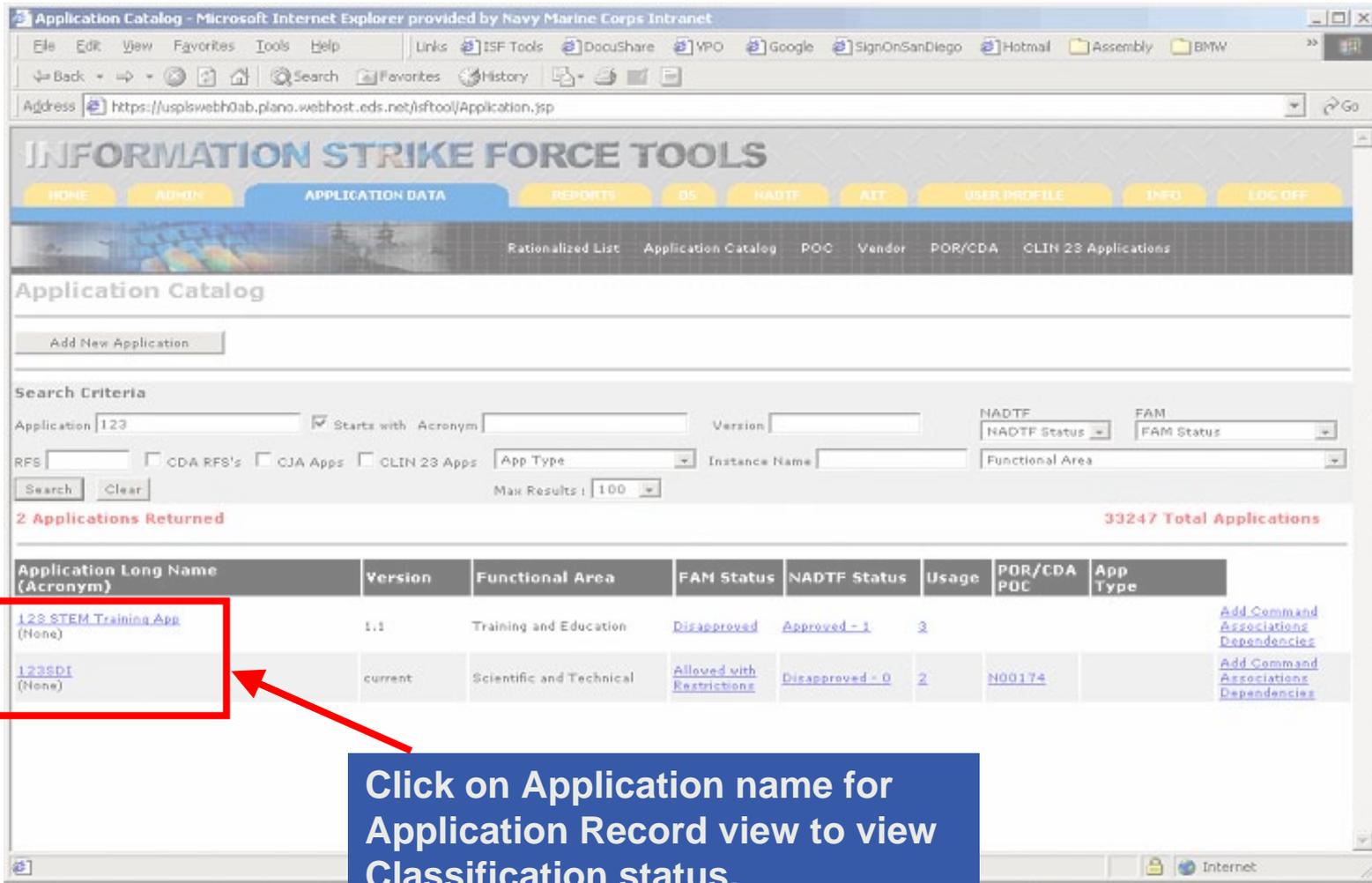
## q **The rules for application to IG-Increment assignment are:**

- ‘NIPRNET only’ applications
  - Can be assigned to the Unclassified Increments
  - Cannot be assigned to the Classified Increment
- ‘SIPRNET only’ applications
  - Cannot be assigned to the Unclassified Increments
  - Can be assigned to the Classified Increment
- ‘NIPRNET and SIPRNET’ applications
  - Can be assigned to the Unclassified Increments
  - Can be assigned to the Classified Increment

- **If the application already has an RFS in ISF Tools for the Command for the unclassified increment(s), another RFS does not need to be submitted.**
- **When the application is assigned to the ‘Classified’ Increment, the RFS# and its AIT Certification information follows the assignment. The RFS for an unclassified application can be used for the Classified side, and vice versa. There is no difference between an unclassified RFS and a Classified RFS, they are the same one.**
- **The ‘re-use’ of an unclassified RFS for the classified instance was a key strategy in the design.**

- α **The Classification Code value for an application can be changed via the Application Catalog page, the rules are:**
  - A. 'NIPRNET only' can be changed to 'NIPRNET and SIPRNET'
  - B. 'NIPRNET and SIPRNET' can be changed to 'NIPRNET only'
  - C. 'SIPRNET only' cannot be changed
  
- α **For Rule B, once LADRA data has been recorded under both unclassified and classified Increments, the Classification Code cannot be changed unless the application is un-assigned from the Classified Increments that contain the LADRA data. Cases for changing these values outside of what is allowed online will be reviewed by FAM and NADTF on per application basis (the ISF Tools System Admin or DBA will make the change).**

# Classification Code – Change Roles



Application Catalog - Microsoft Internet Explorer provided by Navy Marine Corps Intranet

Address: https://usplswebh0ab.plano.webhost.eds.net/isftool/Application.jsp

## INFORMATION STRIKE FORCE TOOLS

HOME ADMIN **APPLICATION DATA** REPORTS DS NADTF ATT USER PROFILE INFO LOG OFF

Rationalized List Application Catalog POC Vendor POR/CDA CLIN 23 Applications

### Application Catalog

Add New Application

**Search Criteria**

Application: 123  Starts with Acronym:  Version:  NADTF: NADTF Status  FAM: FAM Status

RFS:   CDA RFS's  CJA Apps  CLIN 23 Apps  App Type:  Instance Name:  Functional Area:

Search Clear Max Results: 100

2 Applications Returned 33247 Total Applications

Application Long Name (Acronym)	Version	Functional Area	FAM Status	NADTF Status	Usage	POR/CDA POC	App Type	
<a href="#">123 STEM Training App (None)</a>	1.1	Training and Education	<a href="#">Disapproved</a>	<a href="#">Approved - 1</a>	3			<a href="#">Add Command Associations</a> <a href="#">Dependencies</a>
<a href="#">123SDI (None)</a>	current	Scientific and Technical	<a href="#">Allowed with Restrictions</a>	<a href="#">Disapproved - 0</a>	2	N00174		<a href="#">Add Command Associations</a> <a href="#">Dependencies</a>

Click on Application name for Application Record view to view Classification status.

## ☐ **Workbook Report**

- No changes were made to this report because it does not present IA data.

## ☐ **DAA Report**

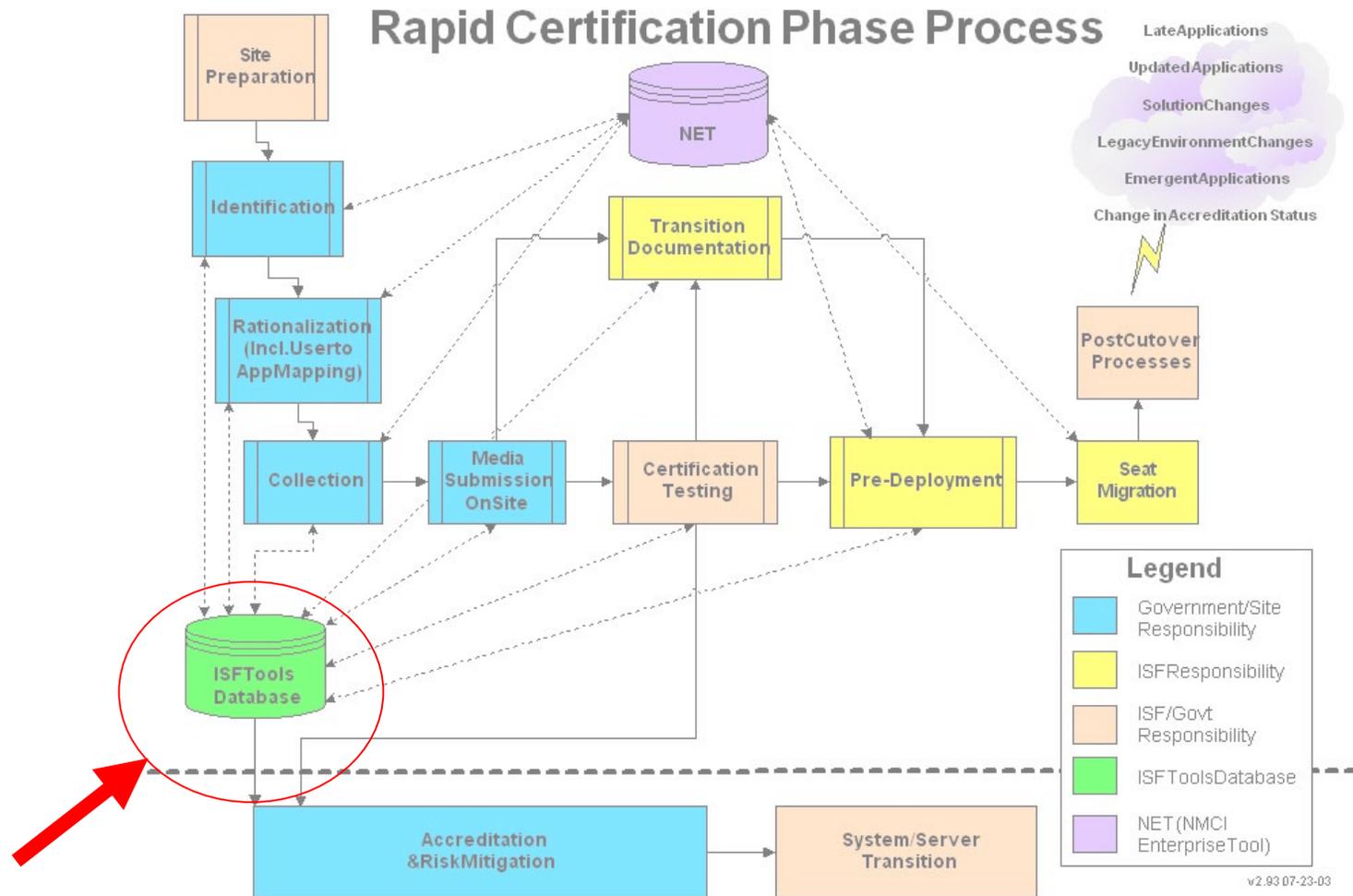
- IA data is presented on the DAA Report, however, no changes were made to it, because the IA data was disallowed from being entered for classified applications on the ADS pages. The report shows blank columns for this data. The Simple/Complex choice will be presented if it was selected.

## ☐ **There are no other reports that present IA data.**

- α **Classified applications are managed by the same ISF Tools web application as unclassified applications.**
- α **Classified applications are managed via the ‘Classified Increment’ of an Implementation Group.**
- α **The ‘Classification Code’ of an application controls which Increments of an IG an application can be assigned to.**
- α **RFS’s are shared between the ‘unclassified’ and ‘Classified’ Increments. There is no need to submit two.**
- α **Information Assurance (IA) data is disallowed from being entered for applications assigned to the ‘Classified’ Increment.**

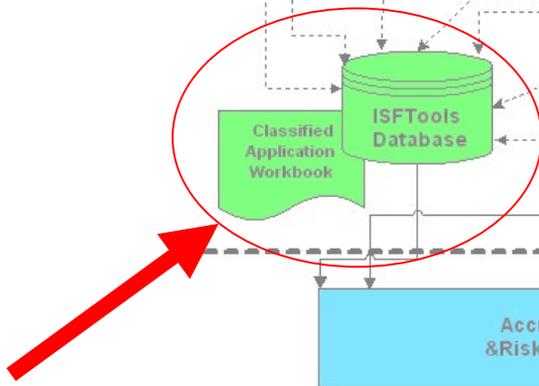
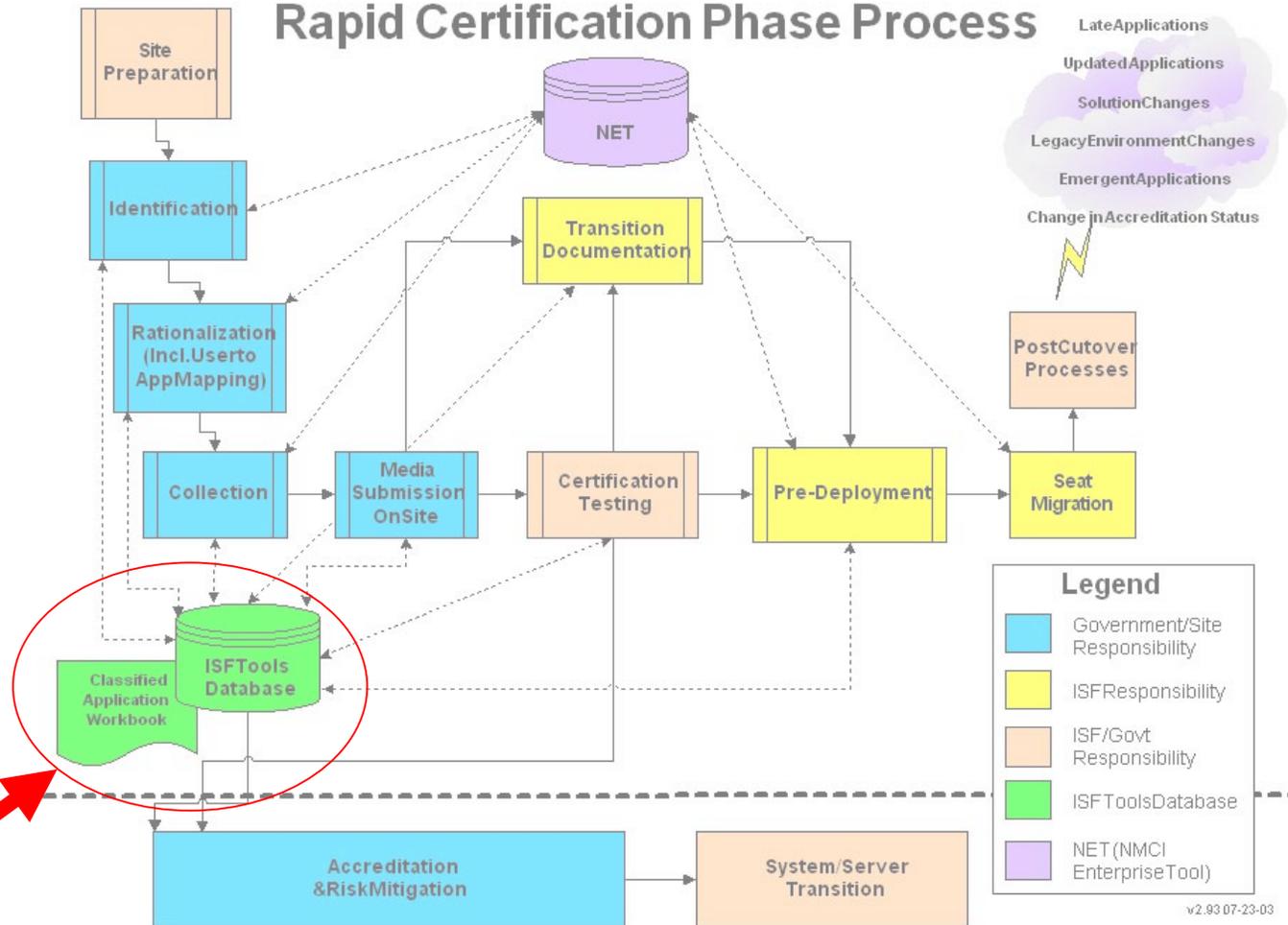
# Testing Process Overview

# Unclassified Rapid Certification Phase Process



# Classified Rapid Certification Phase Process

## Rapid Certification Phase Process



## ☒ **Requirements:**

- Secure facilities/storage
- Custody
- Personnel clearances
- All available security reference materials for EDS LADRA Site Solutions Team

## ☒ **Classified Test Seats**

- Planning needs to be done for a secure test area for LDSD&T and LADRA test seats

## ☒ **SIPRNET access**

- The site may need to provide SIPRNET access to the EDS team members (when requested) for secure e-mail if needed.

α **The site's ISSM/ISSO is responsible for:**

- Identification of which applications can be in ISF Tools
- Distribution of media to local site test locations or to NMCI Classified Application Test lab
- Verification of personnel and access to testing location
- Storage of Documentation and Media
- Review of site's Classified Legacy Application Workbook if manual rationalization process is being followed

α **The site's Classified Legacy Applications Workbook will be created for those applications that cannot be entered into ISF Tools**

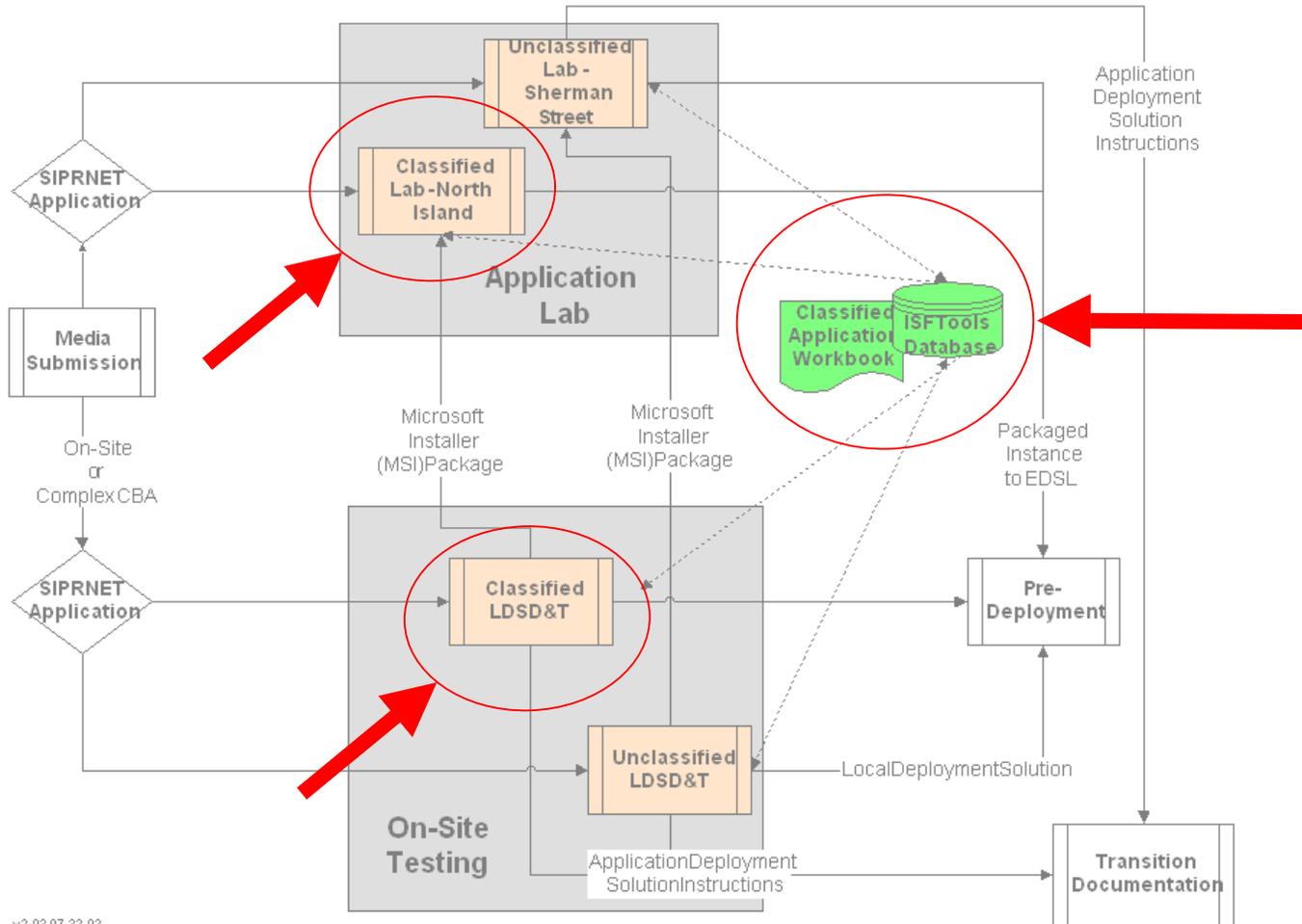
- Each application will be pre-assigned a CRFS number.
- The workbook will then be sent to the site by the EDS Classified Product Delivery Analyst using the same handling that was used by the site.
- Sites will download and use the Classified RFS form for all classified application submissions to EDS, and will use the pre-assigned CRFS number.
- The Classified Product Delivery Analyst will work with sites and provide NMCI Certification/Validation status.

- q **Sites will create Application Mapping (UTAM).**
  - Same process as followed in Unclassified Rapid Process
- q **Sites will identify peripherals, associated drivers and software.**
  - Same process as followed in Unclassified Rapid Process
- q **Sites and EDS will participate in site-specific Workbook Reconciliation meetings.**

- α **The Collection process is a Government responsibility.**
  - Secure Handling procedures, Personnel Security Clearances, Custody, and Storage are all factors that have to be addressed.
- α **Application media and supporting documentation must be collected for submission to EDS as documented in the LATG**
- α **Classified legacy applications require the following:**
  - The completed RFS
  - Media and License Validation
  - Installation Instructions and Test Scripts
  - Network Diagram (desktop-to-server connectivity)
  - Test Plan



# Testing Process



v2.93 07-23-03

# Testing Flow – Part 1

## Audit Inputs

- RFS
- Media
- License Key (If Required)
- Installation Instructions (Optional)
- Engineering Review Questionnaire (Optional)
- Connectivity Requirements (Optional)
- Configuration Requirements (Optional)
- Testing Scripts/Plans (Optional)
- User To Application Mapping (Optional)

## CBA Inputs

- RFS
- Media
- Tested Application or Package
- Installation Instructions
- Configuration Instructions
- Updated ISF Tools Status and Notes
- Updated Shared Folder for Application
- EtherPeak Trace Files
- Updated DAA Report
- License Key (If Required)
- Engineering Review Questionnaire (Optional)
- Testing Scripts/Plans (Optional)
- User To Application Mapping (Optional)



Certification By Association



Generate Letter and Deploy

## Failed Audit

- Failure Report
- Updated ISF Tools Status and Notes
- Shared Folder for Application
- DAA Report Updated

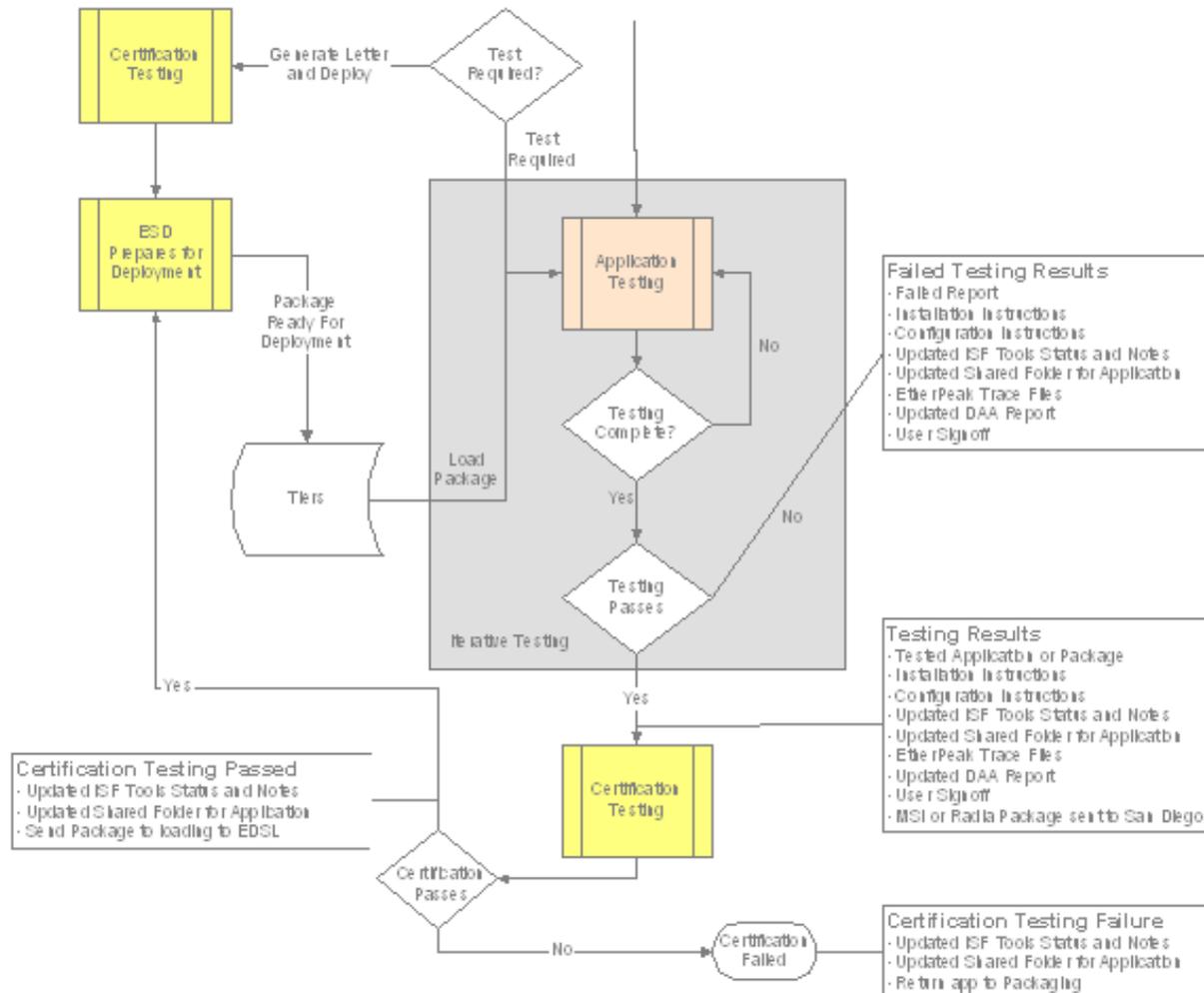
## Audit Results

- Audited Application Package
- Updated ISF Tools Status and Notes
- Shared Folder for Application
- Recommend Packaging Method

## Packaging Results

- Application Package Solution
  - Radia
  - Advance Package (MSI)
  - Installation Media
- Installation Instructions
- Configuration Instructions
- Updated ISF Tools Status and Notes
- Updated Shared Folder for Application

# Testing Flow – Part 2



- α **Classified NMCI Information Assurance (IA)**
  - NO IA DATA IS RECORDED IN ISF TOOLS
  - Manual IA data is recorded and maintained at the site
  - Process is mostly similar to the Unclassified IA process except for the Boundary 2 and Boundary 3 (COI)
  - There is no B2 or B3 within the SIPRNET
  
- α **The Enterprise Boundary 1 (B1) and Boundary 4 (B4) or Group Policy Object (GPO) are utilized in the Classified NMCI architecture.**

## q **Paul Halpin is the Classified Product Delivery Analyst.**

- Assists sites in the management of Manual Classified Workbooks
- NIPNET email address: [paul.halpin@nmci-isf.com](mailto:paul.halpin@nmci-isf.com)
- SIPRNET email address: [paul.halpin@nmci.navy.smil.mil](mailto:paul.halpin@nmci.navy.smil.mil)

- The address for sending classified media or classified information is:  
Javier Berrellez (NMCI-ISF Security)  
NAVCOMTELSTA – NMCI  
Attn: NMCI Security Room 246  
Bldg. 1482 Read Rd.  
Naval Air Station North Island  
San Diego, CA 92135

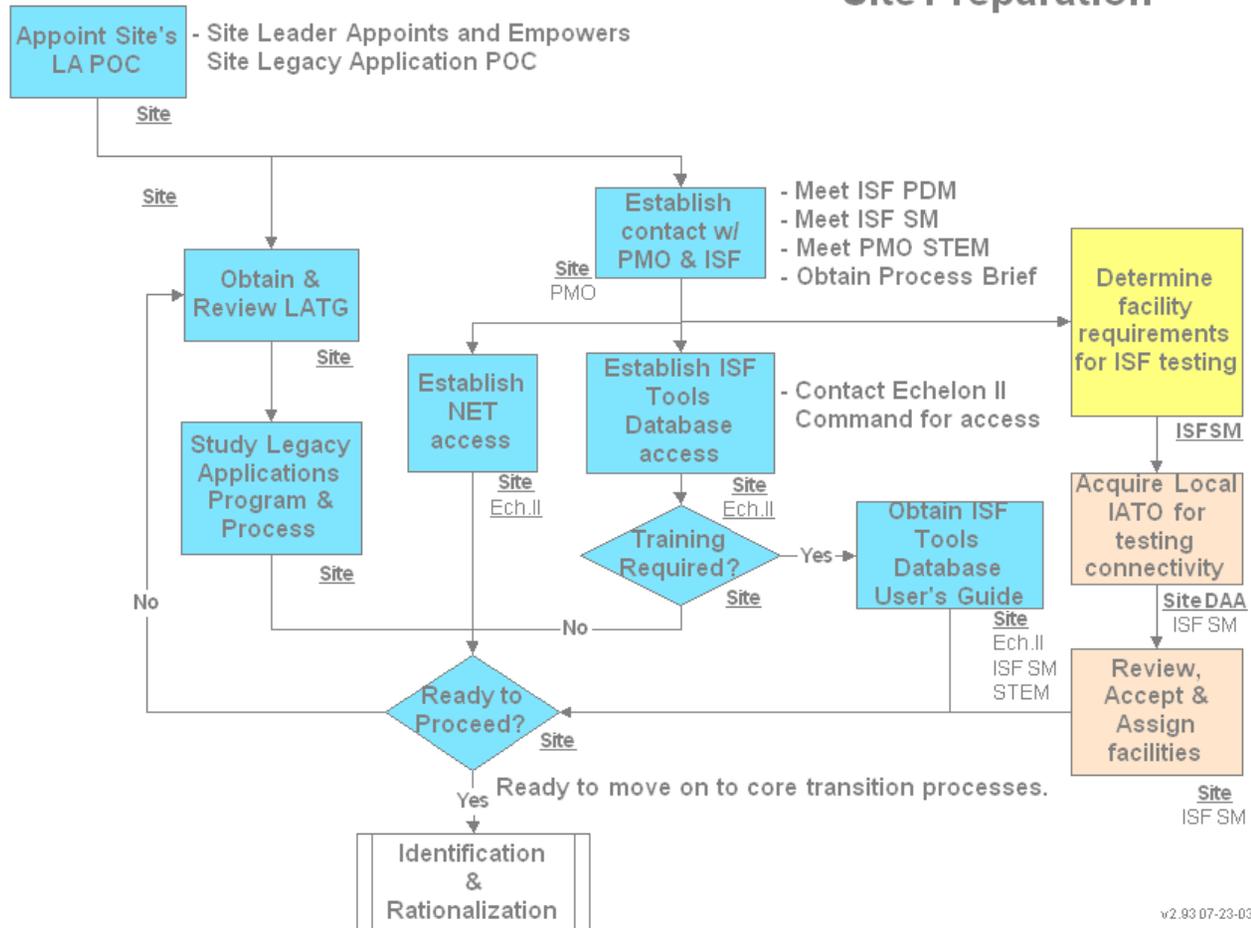
## q Any questions or concerns can be addressed to

- Mike Osnowitz – [mike.osnowitz@eds.com](mailto:mike.osnowitz@eds.com)
- Steve Strull – [steven.strull@eds.com](mailto:steven.strull@eds.com)
- Paul Halpin - [paul.halpin@nmci-isf.com](mailto:paul.halpin@nmci-isf.com)
- Javier Berrellez - [javier.berrellez@nmci-isf.com](mailto:javier.berrellez@nmci-isf.com)

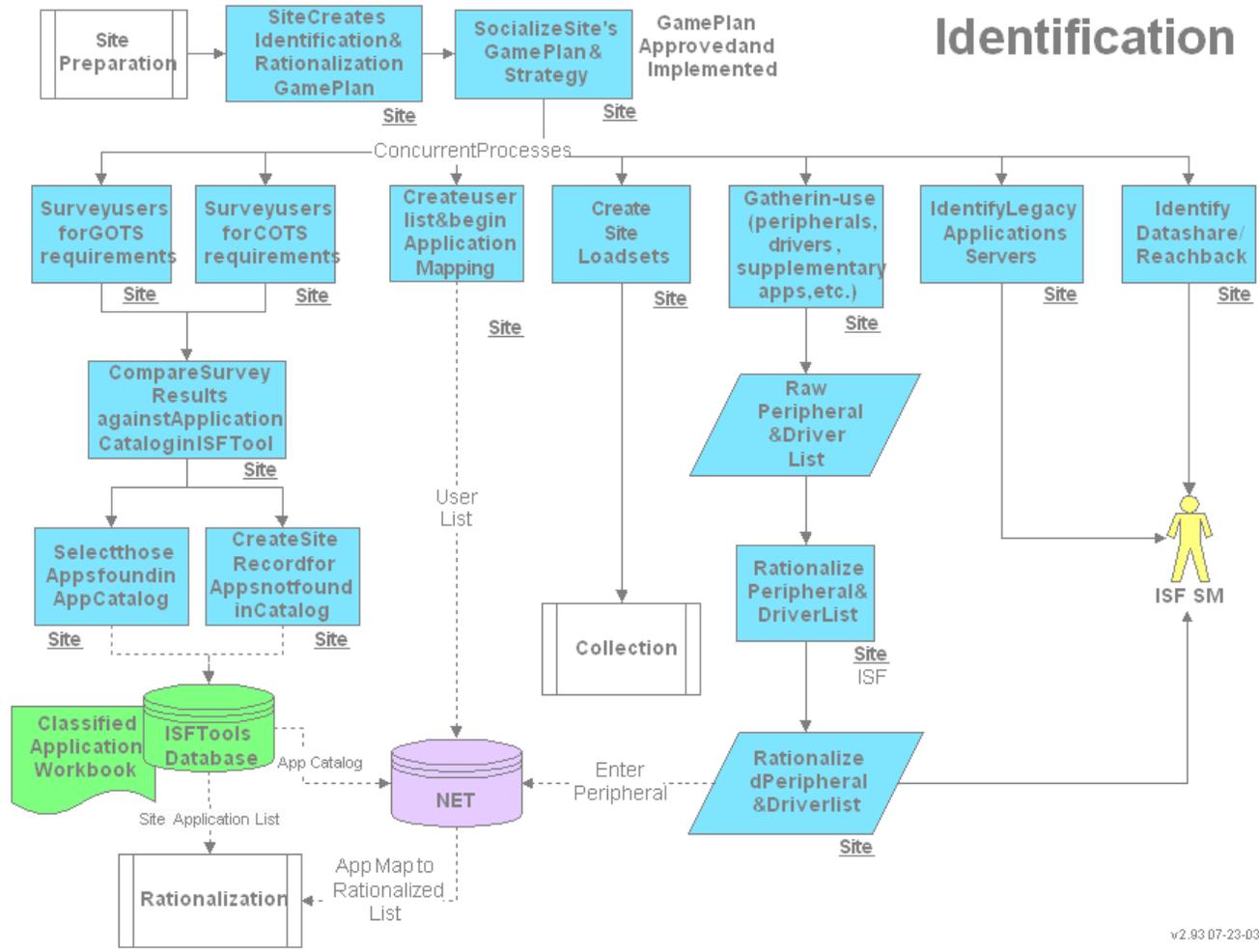


## **Backup Slides**

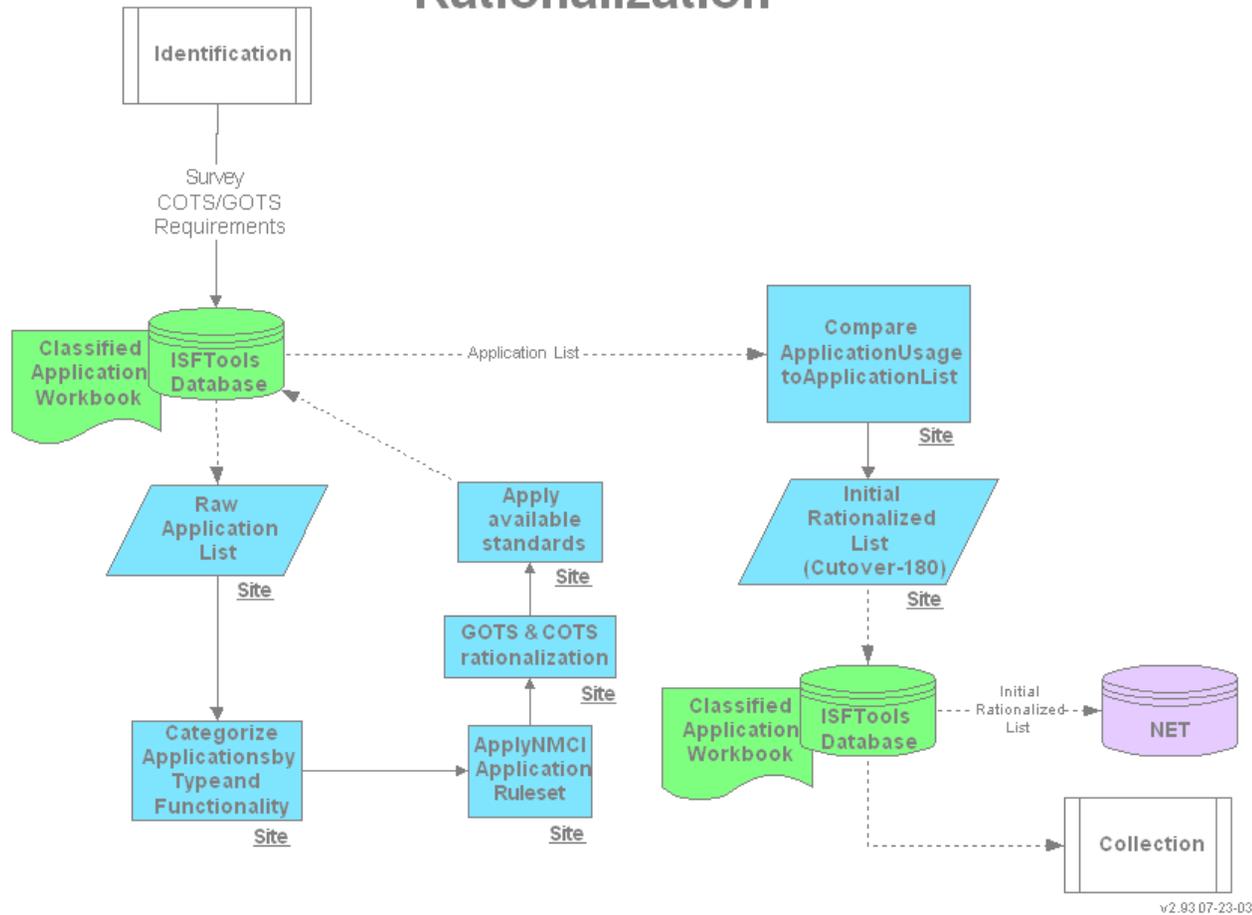
## Site Preparation

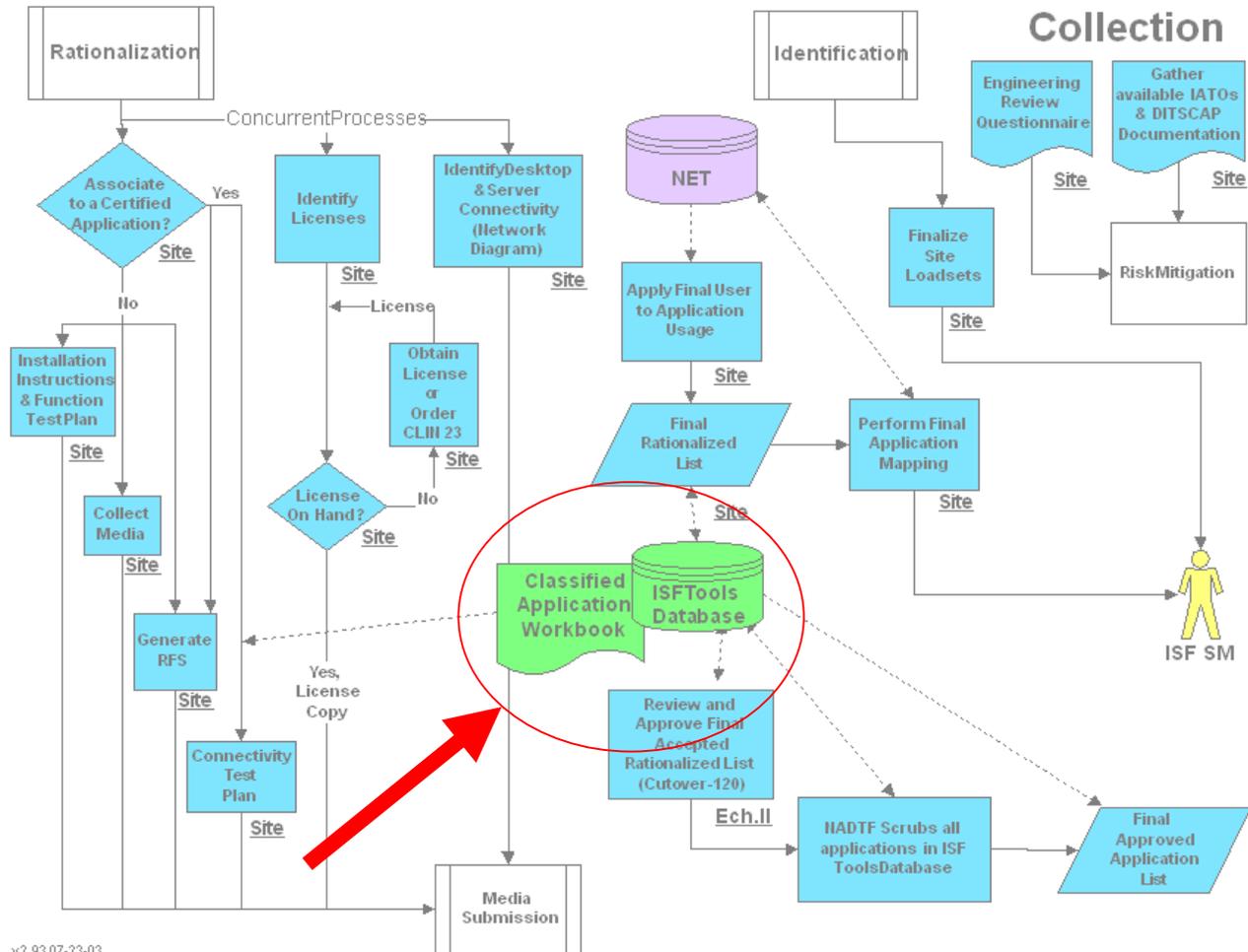


# Identification



## Rationalization





v2.93 07-23-03