**Scan Results Processor (SRP)**

**USER’S MANUAL**

*Robert Sakey*

Version 4.0.15: April 18, 2017

**Revision Sheet**

|  |  |  |  |
| --- | --- | --- | --- |
| **Release No.** | **Date** | **Revision Description** | **Author** |
| 1.00 | 10/28/2010 | Initial Release | Robert Sakey and Jeremy Silverstein |
| 1.01 | 11/30/2010 | Split Database into Front End and Back End | Robert Sakey |
| 1.02 | 11/30/2010 | Various Changes | Robert Sakey and Don Biedermann |
| 1.03 | 1/3/2011 | Various Changes | Robert Sakey |
| 1.04 | 1/23/2011 | Various Changes | Robert Sakey |
| 1.05 | 2/6/2011 | Changes in line with new Navy templates | Robert Sakey |
| 1.06 | 3/16/2011 | Minor changes for usability | Robert Sakey |
| 2.00 | 5/3/2011 | Added code to automatically update back end and front end | Robert Sakey |
| 2.0.1 | 5/17/2011 | Bug fixes | Robert Sakey |
| 2.0.2 | 6/13/2011 | Minor bug fixes and changes to inherited findings | Robert Sakey |
| 2.0.3 | 8/31/2011 | FISMA form and report plus minor bug fixes | Robert Sakey |
| 2.0.4 | 11/10/2011 | Minor bug fixes | Robert Sakey |
| 2.0.5 | 1/3/2012 | Major and minor bug fixes; Scan Results Form closes faster if no changes made; Updated install instructions | Robert Sakey |
| 2.0.6 | 3/29/2012 | Major changes and bug fixes | Robert Sakey |
| 2.0.7 | 3/30/2012 | Minor fix to change single quotes to double quotes for Validation Report Vulnerabilities | Robert Sakey |
| 2.0.8 | 4/5/2012 | Fix to Validation Report to not add vulnerabilities to Vulnerability field of N/A IA controls | Robert Sakey |
| 2.0.9 | 9/24/2012 | STIG Viewer Import | Robert Sakey |
| 3.0.0 | 1/23/2013 | eMASS Risk Assessment form | Robert Sakey |
| 3.0.1 | 3/13/2013 | eMASS POA&M Import | Robert Sakey |
| 3.0.2 | 9/8/2014 | Bug fixes | Robert Sakey |
| 3.0.3 | 11/19/2014 | Replaced Vulnerator with ACAS as Import Types | Robert Sakey |
| 3.0.4 | 11/19/2014 | Bug fixes and some new features | Robert Sakey |
| 4.0.0 | 5/4/2015 | Major changes including major bug fixes and new features | Robert Sakey |
| 4.0.1 | 7/17/2015 |  | Robert Sakey |
| 4.0.2 | 1/3/2016 | Changes to MainGui, eMASS POA&M Import and bug fixes | Robert Sakey and Scott Merrill |
| 4.0.3 | 4/13/2016 | Minor changes | Robert Sakey |
| 4.0.4 | 6/28/2016 | Added All Scan Results Form | Robert Sakey |
| 4.0.5 | 7/25/2016 | Major changes including All Scans Form, Selecting Back End Database, Software, Hardware and PPS forms/reports | Robert Sakey |
| 4.0.6 | 8/03/2016 | Major revisions to Scan Results Form and All Scan Results Form | Robert Sakey |
| 4.0.7 | 8/26/2016 | Minor updates | Robert Sakey |
| 4.0.8 | 11/2/2016 | Major Updates; removed All Hosts Checkbox; | Robert Sakey |
| 4.0.9 | 1/26/2017 | Major Updates | Robert Sakey |
| 4.0.10 | 2/8/2017 | Added Baseline | Robert Sakey |
| 4.0.11 | 2/9/2017 | Report fixes | Robert Sakey |
| 4.0.12 | 3/28/2017 | Updated Hosts in Hosts table | Robert Sakey |
| 4.0.13 | 4/06/2017 | Added import from STIG Viewer 2.5.X | Robert Sakey |
| 4.0.14 | 4/7/2017 | Changed STIG Viewer Import to automatically test for version | Robert Sakey |
| 4.0.15 | 4/18/2017 | Minor fixes | Robert Sakey |

**TABLE OF CONTENTS**

[1 Introduction 6](#_Toc479331518)

[1.1 Purpose 6](#_Toc479331519)

[1.2 Scope 6](#_Toc479331520)

[2 Getting Started 6](#_Toc479331521)

[2.1 System Requirements 6](#_Toc479331522)

[2.2 Scan Results Processor Contents and Description 6](#_Toc479331523)

[2.3 Installation 7](#_Toc479331524)

[2.3.1 Install Scan Results Processor 7](#_Toc479331525)

[2.3.2 Copy SRP to Working Directory 7](#_Toc479331526)

[2.3.3 Windows 7 7](#_Toc479331527)

[2.3.4 Microsoft Office 2007 8](#_Toc479331528)

[2.4 Starting the Scan Results Processor 8](#_Toc479331529)

[2.5 Setting up the Database 9](#_Toc479331530)

[3 Operations 11](#_Toc479331531)

[3.1 Vulnerator 11](#_Toc479331532)

[3.2 Import Data 12](#_Toc479331533)

[3.3 Scan Results 15](#_Toc479331534)

[3.3.1 Viewing Vulnerabilities 15](#_Toc479331535)

[3.3.2 Updating Vulnerabilities 16](#_Toc479331536)

[3.3.3 Dealing with Vulnerabilities that are Open on one Host and Closed on Another 17](#_Toc479331537)

[3.3.4 Scan Results Report 17](#_Toc479331538)

[3.3.5 Closing the Scan Results Form 17](#_Toc479331539)

[3.3.6 Scan Summary 18](#_Toc479331540)

[3.4 More Imports 19](#_Toc479331541)

[3.5 Implementation Plan 20](#_Toc479331542)

[3.6 Validation Plan 21](#_Toc479331543)

[3.7 Validation Report 22](#_Toc479331544)

[3.8 Plan of Actions and Milestones (POA&M) 25](#_Toc479331545)

[3.9 DIACAP Scorecard 26](#_Toc479331546)

[3.10 Forms & Reports 27](#_Toc479331547)

[3.10.1 Software List 27](#_Toc479331548)

[3.10.2 Multiple Hosts Findings Report 28](#_Toc479331549)

[3.10.3 Vulnerabilities by IA Controls Report 29](#_Toc479331550)

[3.10.4 Vulnerability Count Report 30](#_Toc479331551)

[3.10.5 Mitigated Vulnerabilities List 30](#_Toc479331552)

[3.10.6 Inheritance List 30](#_Toc479331553)

[3.10.7 Test Plan 31](#_Toc479331554)

[3.10.8 Implementation Plan for Export 31](#_Toc479331555)

[3.10.9 Validation Report for Export 31](#_Toc479331556)

[3.10.10 DIACAP Scorecard for Export 32](#_Toc479331557)

[3.10.11 FISMA Report 32](#_Toc479331558)

[3.10.12 N/A IA Controls for POA&M 33](#_Toc479331559)

[3.10.13 eMASS Risk Assessment Report 33](#_Toc479331560)

[3.10.14 eMASS POA&M Import 33](#_Toc479331561)

[3.10.15 Scans Form 33](#_Toc479331562)

[3.10.16 CD Totals 33](#_Toc479331563)

[4 Troubleshooting 34](#_Toc479331564)

[5 Points of Contact 34](#_Toc479331565)

[6 Revision History 34](#_Toc479331566)

[6.1 1.00 34](#_Toc479331567)

[6.2 1.01 34](#_Toc479331568)

[6.3 1.02 34](#_Toc479331569)

[6.4 1.03 35](#_Toc479331570)

[6.5 1.04 35](#_Toc479331571)

[6.6 1.05 35](#_Toc479331572)

[6.7 1.06 36](#_Toc479331573)

[6.8 2.00 36](#_Toc479331574)

[6.9 2.0.1 37](#_Toc479331575)

[6.10 2.0.2 37](#_Toc479331576)

[6.11 2.0.3 37](#_Toc479331577)

[6.12 2.0.4 37](#_Toc479331578)

[6.13 2.0.5 38](#_Toc479331579)

[6.14 2.0.6 38](#_Toc479331580)

[6.15 2.0.7 39](#_Toc479331581)

[6.16 2.0.8 39](#_Toc479331582)

[6.17 2.0.9 39](#_Toc479331583)

[6.18 3.0.0 39](#_Toc479331584)

[6.19 3.0.1 40](#_Toc479331585)

[6.20 3.0.2 40](#_Toc479331586)

[6.21 3.0.3 40](#_Toc479331587)

[6.22 3.0.4 41](#_Toc479331588)

[6.23 4.0.0 41](#_Toc479331589)

[6.24 4.0.1 42](#_Toc479331590)

[6.25 4.0.2 42](#_Toc479331591)

[6.26 4.0.3 43](#_Toc479331592)

[6.27 4.0.4 43](#_Toc479331593)

[6.28 4.0.5 43](#_Toc479331594)

[6.29 4.0.6 44](#_Toc479331595)

[6.30 4.0.7 44](#_Toc479331596)

[6.31 4.0.8 44](#_Toc479331597)

[6.32 4.0.9 45](#_Toc479331598)

[6.33 4.0.10 45](#_Toc479331599)

[6.34 4.0.11 45](#_Toc479331600)

[6.35 4.0.12 45](#_Toc479331601)

[6.36 4.0.13 45](#_Toc479331602)

[6.37 4.0.14 45](#_Toc479331603)

# Introduction

The information assurance (IA) community uses numerous tools to test, scan, document, and present an information system’s security posture under the Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP). The Scans Results Processor (SRP) provides an automated means to process, document, and present the raw data captured in the various IA testing, scans, and checklists. SRP provides the processed data in the format and on the forms required in DIACAP.

## Purpose

This handbook details the procedures necessary for the use and operation of the SRP tool.

## Scope

The original SRP was a government owned tool that may be used by any DoD government entity at no charge. Following in that tradition, this modification to the SRP is available free of charge. No license is required. The tool is designed around the Navy DIACAP process and provides data in established forms and formats.

# Getting Started

## System Requirements

* Microsoft Office 2010 or newer
  + Scan Results Processor database built with Access 2010 and may require work-arounds to work in Access 2007
* STIG Viewer (optional)
  + Tool for aggregation of security findings for systems
  + Located on the iase.disa.mil website
* ACAS (optional)
  + Tool for scanning Windows, Linux and UNIX computers
  + Located on the iase.disa.mil website
* 100 MB of free hard drive space
  + Capacity to host SRP files as well as scan data
  + Installation requires 20 MB of free hard drive space

## Scan Results Processor Contents and Description

* Scan Results Processor.accdb
  + Front end database file used for importing, processing, and display of scan data.
* Scan Results Processor be.accdb
  + Back end database file used for storing scan data.
* POAM.xlsx.
  + Template spreadsheet to receive Plan of Actions and Milestones data from SRP.
* ManualScansTemplate.xlsx
  + Template spreadsheet for inputting Manual Scan data.

## Installation

### Install Scan Results Processor

Run the executable file called Scan Results Processor.exe. Two separate databases with different file names will be created, a front end and a back end database. The front end database is called Scan Results Processor.accdb and the back end database is called Scan Results Processor be.accdb. These two database files will be placed in the folder named C:\Scan Results Processor. The databases can be renamed later for convenience. It is suggested that the following convention be used for naming the front and back end databases. Front End = “Name.accdb”. Back End = “Name be.accdb” Don’t forget to put a space between the “name” and the “be” parts.

### Copy SRP to Working Directory

The Scan Results Processor can be run from the installation folder or a different folder. For configuration management reasons an instance of the SRP should be copied to a different working directory. It is recommended that the SRP folder be set as a Microsoft Trusted Location. Separate versions of the SRP can be installed for each project in separate directories. For example, if you have two versions of a system that would produce two separate POA&Ms, etc. The POAM template should be copied to each working directory. When upgrading to a newer version of SRP, make sure to only copy over the front end. The front end database is designed to make changes to the back end database without affecting the already existing data.

\*Note: Do not “move” the database, “Copy” it. This will make it easier to relink the front end and back end databases. If the linked back end database is not found, the front end will attempt to link to a database with the same name plus “ be”.

### Windows 7

If an Update Fail error occurs when opening the database for the first time, do the following:

1. Open the front end Scan Results Database while holding Shift key
2. Click Linked Table Manager from the External Data menu
3. Check the Always prompt for new location check box
4. Click Select All
5. Click OK
6. Select the Location of your back end database
7. Click Open
8. Click OK on the pop up dialog box
9. Click Close on the Linked Table Manager
10. Close the database
11. Reopen the database

If the splash screen appears with a Security Warning behind it, do the following:

1. Close the Splash Screen
2. Click Enable Content on the Security Warning
3. Click Setup on the MainGui
4. Click the Relink Database button
5. Follow steps 3 through 11 above

\*\*Note: Sometimes it may be necessary to place the database location in the list of “Trusted Locations”. From the options menu, click Trust Center then the Trust Center Settings button. Click Trusted Locations then Add New Locations.

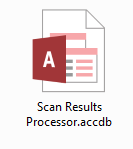
### Microsoft Office 2007

If you are trying to open the database with Microsoft Office 2007 and are encountering issues, do the following:

1. Create a new blank Access database
2. Delete the default table
3. Click External Data 🡪 Import & Link 🡪 Access
4. Browse to the front end database (the one without the “be” in it)
5. Select Import tables, etc.
6. Click Ok
7. For each of the tabs on the Import Objects box, click Select All
8. Then click OK
9. When complete, Go to File 🡪 Options 🡪 Current Database 🡪 Display Form and enter frm\_Splash
10. Make sure that Overlapping Windows is selected in Document Window Options
11. Optionally enter an Application Title to appear on the title bar of the database.

## Starting the Scan Results Processor

* Navigate to the location of the SRP in the working directory.
* Double-click the “Scan Results Processor.accdb” icon.

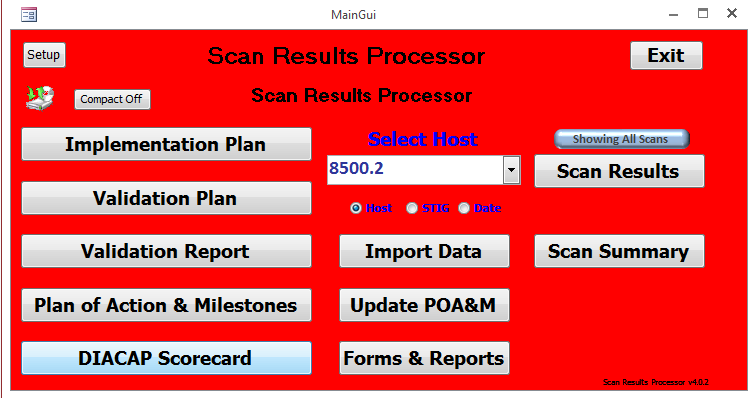


Example of the Scan Results Processor icon

When first opened, the database will execute an update of the back end database if any changes have been made. Click the Yes button and the back end database will update. If there are a lot of updates, you may see the following screen. 

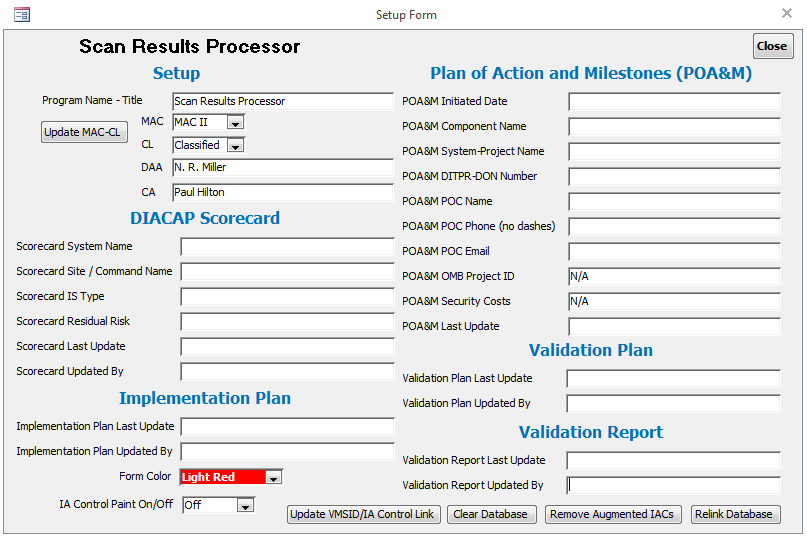
Then Microsoft (MS) Access will execute and open up the database file to the Main graphical user interface (GUI) form.

## Setting up the Database



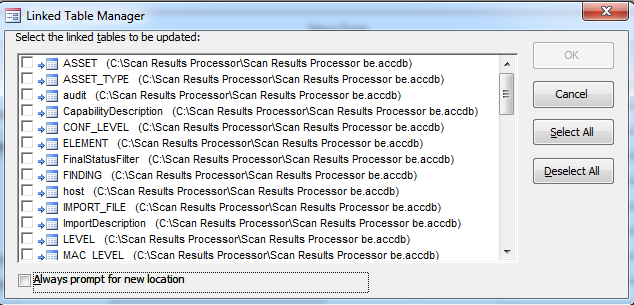
**Example of the Scan Results Processor MainGui Page**

Before importing any data, the database’s general information must be entered. From the MainGui form, click the **Setup** button to open the Defaults Form.



**Example of the Defaults Form**

If the Scan Results Processor was moved or renamed, then the first thing that should be done is to relink the database. The Relink Database button allows the user to link the front end database to the back end database in case the back end database is moved or its name is changed. It is suggested that the user make a copy of the back end database first then either move or rename the copy. Then while the front end database is pointing to the old back end database, the user can change the links.



**Example of the Linked Table Manager Form**

In the Linked Table Manager, select the Always prompt for new location check box. Click the Select All button. Click the OK button. Select the location of the back end database.



After all linked table are successfully refreshed, click the close button.

Click the **Close** button in the upper right to exit and return to the MainGui Form.

\*\*Note: After relinking a database, the user should restart the database before adding any data to the Defaults form.

After returning to the defaults form, the user should enter the necessary information in the appropriate fields. The data in these fields are promulgated to various documents generated by the SRP database.

Upon selecting a Mission Assurance Category (MAC) and Classification Level (CL) click the **Update MAC-CL** button. This triggers a subroutine to generate a list of appropriate Information Assurance Controls (IAC) required to be addressed in the DIACAP documentation.

At the bottom of the Defaults Form are three additional buttons:

* The **Clear Database** button will clear all vulnerability and scan data from the database. This button will not delete any data on the Setup form. It is recommended to Compact and Repair the database after Clearing the Database in order to reset auto-generated scan numbers back to 1
* The **Update VMSID/IA Control Link** button will update a table with VMSID/IA links from STIGs that have been entered in the development database.
* The **Remove Augmented IACs** button will delete any IAC and IA Procedures that were added by the user.
* The **Relink Database** button allows the user to relink the front end database with a back end database.
* The **Form Color** drop down box allows you to change the back color of the MainGui Form.
* The **IA Control Paint On/Off** drop down box allows you to turn paint of the IA Control button On or Off. This allows for the IA Control button text to display red for no IA Controls associated with the vulnerability on the Scan Results form or blue for IA Controls that are N/A. There will be flicker on the Scan Results form when this is turned on. It is recommended to leave this off except when need as the paint function that it is tied to is annoying. You’ll see.

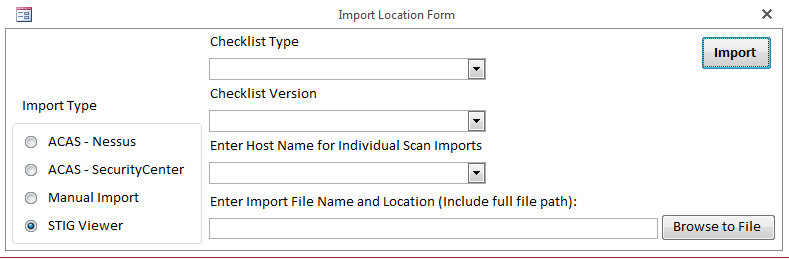
# Operations

## Vulnerator

Vulnerator is no longer supported by the SRP.

## Import Data

To import scan data into SRP, click the **Import Data** button from the MainGui Form. This launches the Import Location Form.



**Example of the Import Location Form**

A radio button allows the user to select between four types of import formats: “**ACAS - Nessus**”, “**ACAS – SecurityCenter**”, “**Manual Import**” and **“STIG Viewer”.** You need to know the following to import a scan:

* ACAS – Nessus Import
  + From Nessus, select a scan
  + From the Export drop down box, select CSV
  + Save the file



* ACAS – SecurityCenter Import
  + From SecurityCenter, select Scanning 🡪 Scan Results
  + Select a scan
  + Click the Report button
  + Select the Detailed Vulnerability Template
    - The Detailed Vulnerability Template is one of four provided on the DoDs ACAS web site
  + Give the export a name and click the Launch button
    - If the report fails, log out of ACAS, log back in and retry
  + Go to Reporting 🡪 Report Results
  + Select the report and click the Download button
  + Save the file
  + The .csv file will appear in you download directory

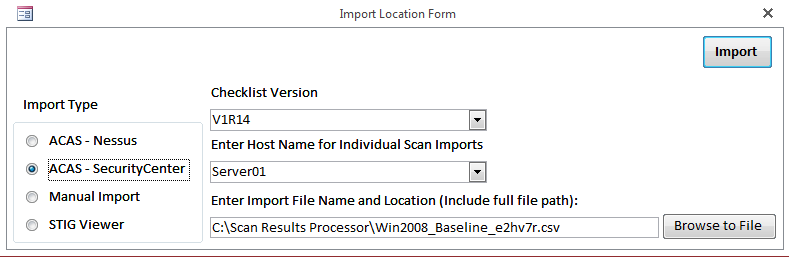




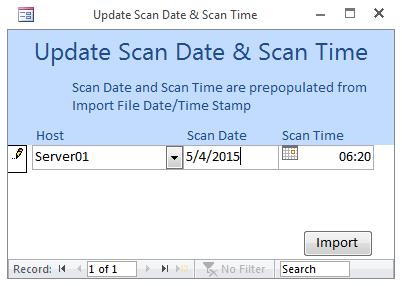


* Manual Import – Use Manual Scan Template saved as Excel Spreadsheet, .xlsx
* STIG Viewer Import –
  + From the Export Menu 🡪 Select CSV File (Excel)
  + Make sure all STIG Items and Checklist Items are checked
  + Click File button to select name and location of file
  + Click Save
  + Click Export button (sometimes it is hidden)
  + A CSV file will be generated
  + File name must be no more than 60 characters maximum
  + File name must have no periods other than the one before the extension

Select the scan data file by clicking the **Browse to File** button and choose the appropriate file (e.g. ManualScans.xlsx). Make sure to set Files of type: to Excel File or XML Files depending on the import type. Then click **Open** to continue back to the Import Location Form. From there click the **Done** button. On the Import Location Form, click the Import button.



The “Update Scan Date & Scan Time” dialog will appear automatically. Updating the scan dates and times for each host included in the scan will be required. Manual Scans will already have the information filled in as it is provided with the template. The date and time will default to the file stamp date and time.



**Example of the Update Scan Date & Scan Time**

The values in the Host, Scan Date and Scan Time fields can be changed at this point. Before you import a scan for a host that is already in the database, make sure that the host name matches the host name already in the database. A combo box in the Host field will allow you to choose any previously imported host name. To import the scan, click the Import button.

If the import goes smoothly, a pop-up dialog will appear expressing a successful import.

With the scan data successfully imported into the SRP database, new reports can be generated and vulnerability management can be performed.

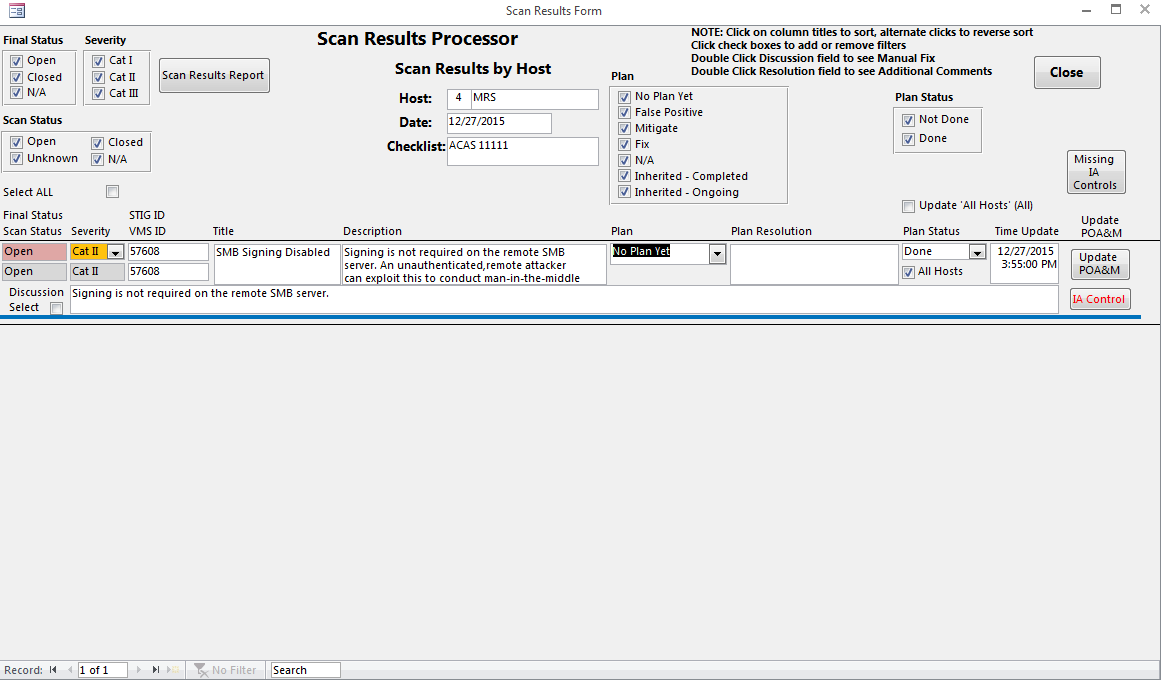
## Scan Results

The Scan Results dialog provides by-host vulnerability management accessibility when host scan data has been successfully imported. To access a particular host’s scan results, select a host from the MainGui’s “**Select Host**” pull-down box and click the **Scan Results** button. To see only the latest scan for a particular host and checklist, click the “**Showing All Scans**” button. It will change to “**Showing Latest Scans**”.

### Viewing Vulnerabilities

From the Scan Results dialog, details regarding the selected host vulnerabilities can be viewed and updated. Each column header is clickable to toggle between ascending and descending sorting.

The view can also be changed by the various checkboxes in the Scan Results header section. By checking and unchecking various boxes, results can be filtered based on the checked criteria.



**Example of the Scan Results Form**

The **All Hosts Update** check box is used to put a check in all the **All Hosts** boxes for each vulnerability line in the form. By checking this box (checked by default), the **All Hosts** box will be checked for all vulnerabilities shown on the form. If it is not desired to have all boxes checked for each vulnerability, then unchecking the **All Hosts Update** will uncheck all **All Hosts** boxes for each vulnerability line. Individual **All Hosts** check boxes can be checked or unchecked at any time. Unchecking the All Hosts checkbox allows you to provide a status for a vulnerability for one host that may be different on another host. For example, if there is an open finding on Server01 and it is closed on Server02, you would want to uncheck the All Hosts checkbox on the scan you want to change, Server01, change Plan Status from Done to Not Done.

### Updating Vulnerabilities

Each vulnerability can be updated with amplifying information. The “Severity”, “Plan”, and “Plan Status” can be selected via drop down combo boxes. The object of this form is to provide a status for the compliance of each vulnerability through the development life-cycle.

The “Plan Resolution” offers a wholly editable textbox to enter specifics as to the mitigation or resolution of each particular vulnerability. The contents of the Plan Resolution field will appear in the comments column of the POA&M and RAR. Double clicking inside the Plan Resolution field will bring up an auxiliary form that allow you to enter the Mitigation Description, Remediation Description, Recommended Corrective Action and Risk Assessment, which are fields on the eMASS Risk Assessment Report (RAR). By double clicking the labels for Mitigation Description and Remediation Description, stock answers will appear.



Additional information in the Manual Fix field can be viewed by double clicking inside the Discussion field.

In addition, the POA&M can be updated with any new vulnerability by clicking the **Update POA&M** button on the this form or the MainGui.

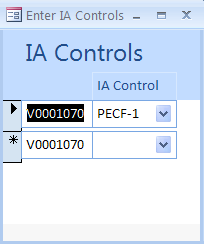
The other textboxes (e.g. “Description”, etc) can also be amplified with further information additional to the pre-populated entries.

Making changes to the Plan and Plan Status fields will change the Final Status field. By changing the Plan field to “False Positive” or “Fix” and then clicking “Done” in the Plan Status field, the Final Status will change to “Closed”. Changing Plan to “N/A” and then selecting “Done” in the Plan Status field will change the Final Status to “N/A”. Changing the Plan field to “Mitigate” or “Inherited” and then selecting “Done” in the Plan Status field will change the Final Status to “Open”, if not already “Open”.

When a new vulnerability is imported, the Plan is set to “No Plan Yet” and the Plan Status is set to “Not Done” even if the Scan Status of the vulnerability is “Closed” or “N/A”. This is to allow the user to enter a Plan Resolution for ALL vulnerabilities as required. Each subsequent imports will inherit the Plan and Plan Status as long as the Scan Status doesn’t change. If a new scan is imported, which has a Closed finding that was previously Open, then the Plan Status will be set to Not Done, giving you the ability to know which previously Open findings need new comments. Just filter for Closed findings with a Plan Status of Not Done.

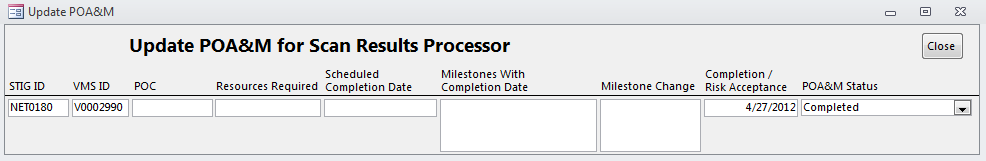
Due to DIACAP requirements, vulnerabilities must be associated with DoDI 8500.2 IACs. Clicking the **IA Control** button brings up a small dialog box from which one or more IA Controls can be associated with a particular vulnerability.

**Warning**: If an Open Vulnerability has no IA Control associated with it, the DIACAP Scorecard and Validation Report will not show it; the POA&M will show it but with an empty field for IA Control.



**Example of the IA Controls Association Dialog Box**

From the Scan Results dialog, Plan of Action and Milestones (POA&M) inputs can be entered via the **Update** button. The inputs to these textboxes will be promulgated to the POA&M generated by the SRP. Changing the Plan field on the Scan Results Form will automatically enter a POA&M Status. For certain Plan values, a Completion / Risk Acceptance Date will also be automatically entered.



**Example of the Update POA&M box**

### Dealing with Vulnerabilities that are Open on one Host and Closed on Another

Open the All Scan Results Form. This will present a list of ALL scan results. Use Control-F to search for the ID of a specific finding. For all instances of the finding, uncheck the All Hosts checkbox. For each host that has a “Closed” finding, change the Plan Status to “Done”. For each host that has an “Open” finding, change the Plan Status to “Not Done”. This will allow the results to display correctly in all reports. Verify that the POA&M status is marked as “Ongoing” by clicking the Update POA&M button for any instance of the finding.

### Scan Results Report

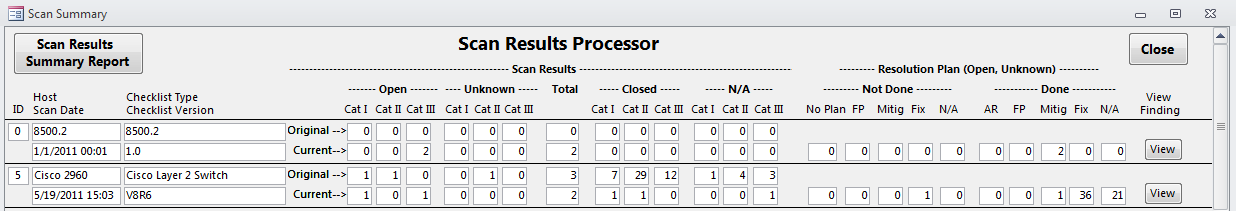
A report showing the vulnerabilities on the Scan Results Form can be viewed by clicking the **Scan Results Report** button.

### Closing the Scan Results Form

The Scan Results Form should always be closed using the **Close** button.

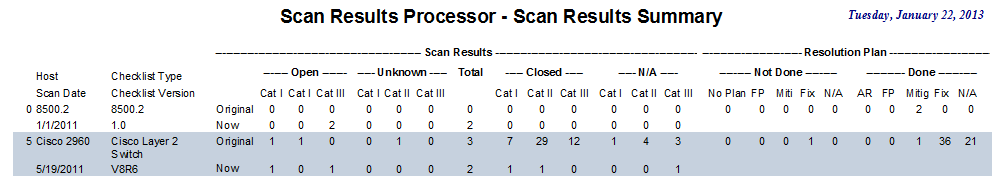
### Scan Summary

From the MainGui, click the **Scan Summary** button. A summary of the number of findings for each scan is shown. The original line will show the vulnerability status upon import. The current line will show the current status for each scan. In order for the current line to be correct for any particular scan, the user must first view that scan from the Scan Results Form.

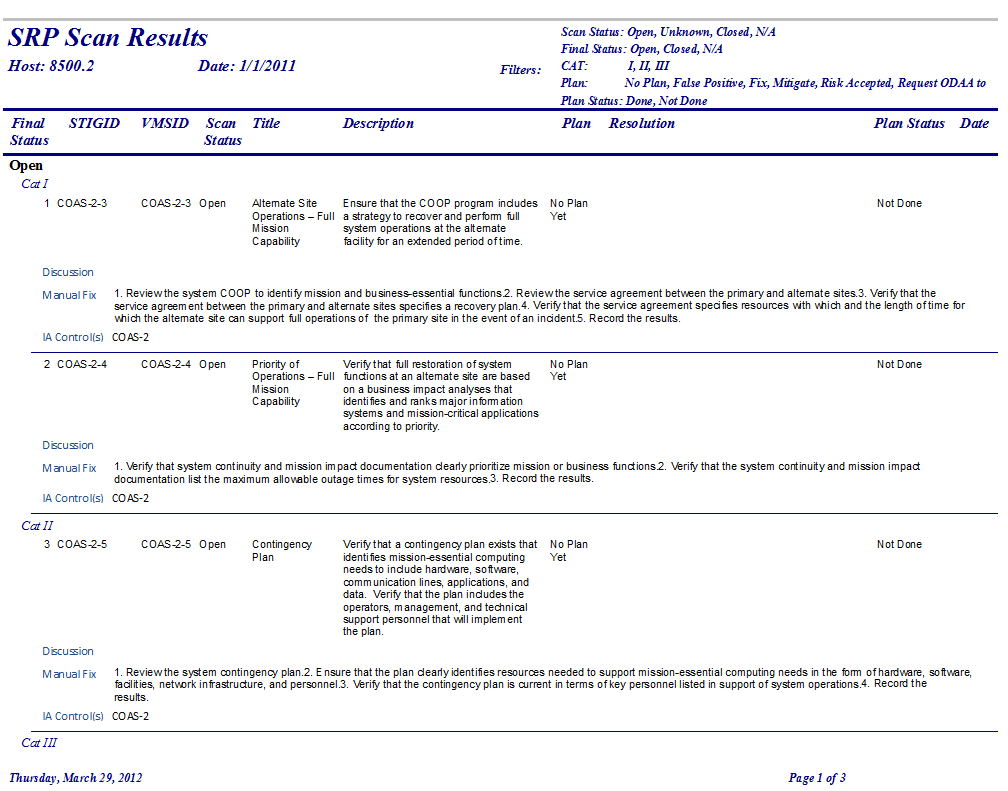


**Example of the Scan Summary Form page**

There are two reports available on the Scan Summary Form, a Scan Summary Report, which shows the contents of the Scan Summary Form and a Scan Results Report, which shows a report similar to the one on the Scan Results Form. This can be accessed by clicking the View button next to each scan.



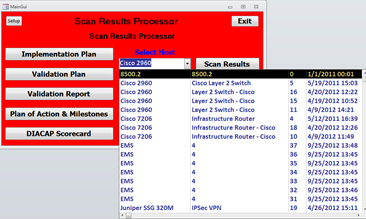
**Example of the Scan Summary Report**



**Example of the Scan Results Report page**

## More Imports

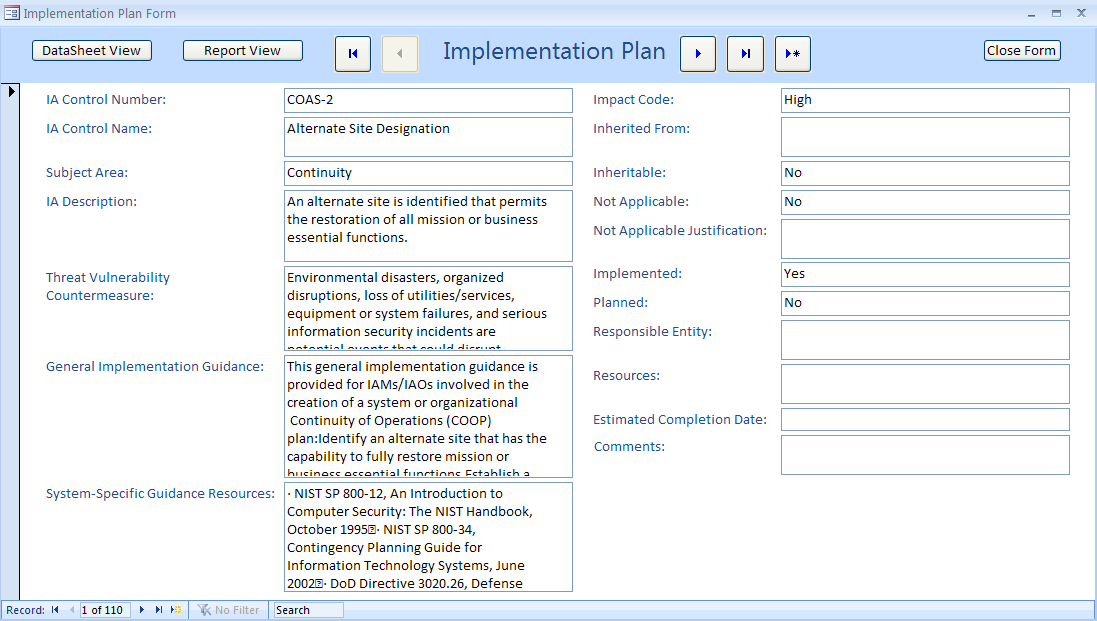
Because it is likely that each host will be scanned multiple times, the SRP allows multiple imports of data for each host. For example, a Gold Disk scan may be imported for a host. After making changes to the status of each vulnerability, another Gold Disk scan is completed and imported into the SRP. When selecting a Host from the Select a Host drop down box on the MainGui, you will notice that the Host is listed more than once with a scan number and a scan date. The latest scan for each host will be listed higher than previous scans.



Select the latest and view the Scan Results. You will notice that some of the information entered previously for each vulnerability is still there, Plan Resolution, for example. The Final Status may change depending upon the results for the new scan. If a Closed finding that was previously marked as Done, will still be marked as Done if it is Closed on the new scan.

## Implementation Plan

The Implementation Plan can be viewed either before or after scan data is imported. Click on the **Implementation Plan** button from the MainGui to view or edit Implementation Plan data. The Implementation Plan Form will show information associated with each IAC filtered by MAC and CL. Some of the information on this form is shown on the DIACAP Scorecard. For a datasheet view of the data, click the **Datasheet View** button. For a printable report, click the **Report View** button.

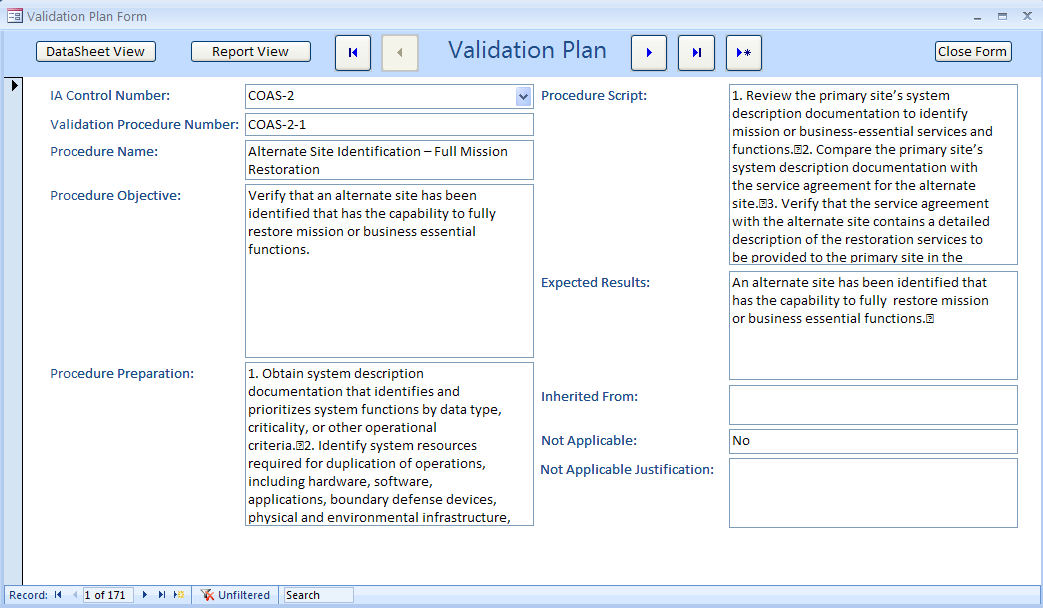


**Example of the Implementation Plan**

**Note**: If the Inherited From, Not Applicable and Not Applicable Justification fields are updated on the Implementation Plan, the Validation Plan and Validation Report will likewise be updated.

## Validation Plan

The Validation Plan can be viewed either before or after scan data is imported. Click on the **Validation Plan** button from the MainGui to view or edit Validation Plan data. The Validation Plan Form will show information associated with each IA Control Procedure filtered by MAC and CL. Some of the information on this form is shown on the DIACAP Scorecard. For a datasheet view of the data, click the **Datasheet View** button. For a printable report, click the **Report View** button.

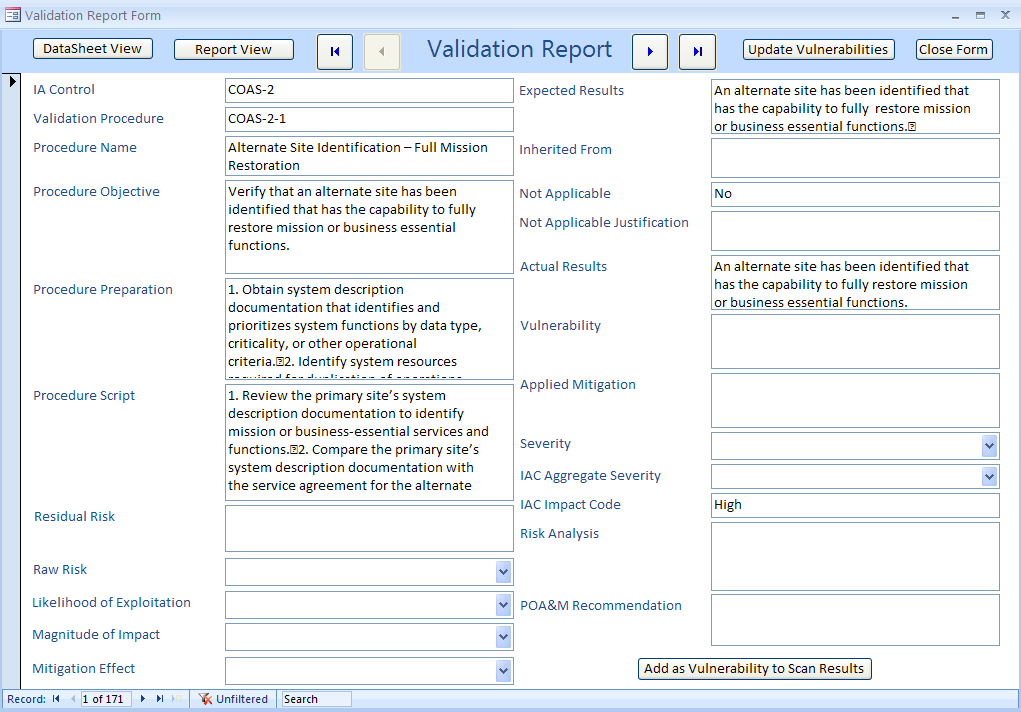


**Example of the Validation Plan**

**Note**: If the Inherited From, Not Applicable and Not Applicable Justification fields are updated on the Implementation Plan, the Validation Plan and Validation Report will likewise be updated.

## Validation Report

The Validation Report can be viewed either before or after scan data is imported. Click on the **Validation Report** button from the MainGui to view or edit Validation Report data. The Validation Report Form will show information associated with each IAC Procedure filtered by MAC and CL. Some of the information on this form is shown on the DIACAP Scorecard and the POA&M. For a datasheet view of the data, click the **Datasheet View** button. For a printable report, click the **Report View** button.



**Example of the Validation Report**

Vulnerability information from the Scan Results can be populated to the Vulnerability field by clicking the **Update Vulnerabilities** button. The Severity field will list the highest Severity of all the vulnerabilities associated with a specific IAC. All other fields must be filled out by the user. The Severity and IAC Aggregate Severity fields contain a drop down menu with CAT I, CAT II, and CAT III for selection.

**Warning**: Due to the lack of a mapping between IAC Procedures and individual vulnerabilities, the SRP will map vulnerabilities to the first procedure associated with each IAC. For example, IAIA-2 has 11 procedures associated with it. If any vulnerabilities are found associated with IAIA-2, the vulnerability text will be automatically added to the first IAIA-2 procedure, IAIA-2-1.

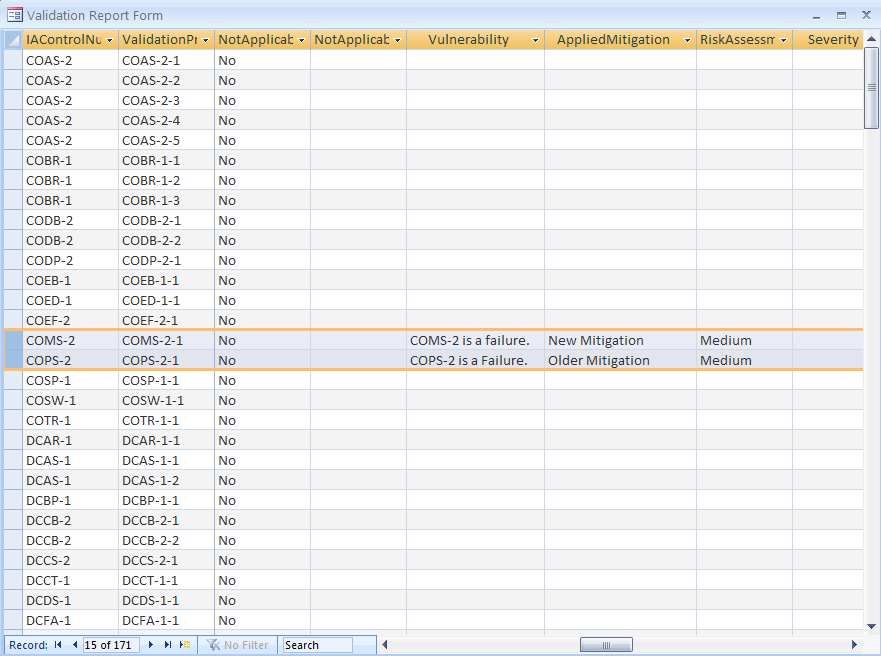
Clicking the **Add as Vulnerability to Scan Results** button will add the procedure as a vulnerability to the scan results with a ScanID of 0 and Host name of 8500.2.

Clicking the **Update Vulnerabilities** button will also add manually created vulnerabilities (8500.2) to the Validation Report, DIACAP Scorecard and POA&M. In addition to the Validation Report, these vulnerabilities will appear on the DIACAP Scorecard and POA&M.

The Residual Risk field contains a drop down menu with High, Medium and Low for selection.

The **IAC Impact Code** field on the Validation Report is set in the **Impact Code** field on Implementation Plan by default.

All other fields should be filled out for any IAC procedure with data in the vulnerability field as it is used to populate the POA&M and Validation Report.



**Example of the Validation Report Form**

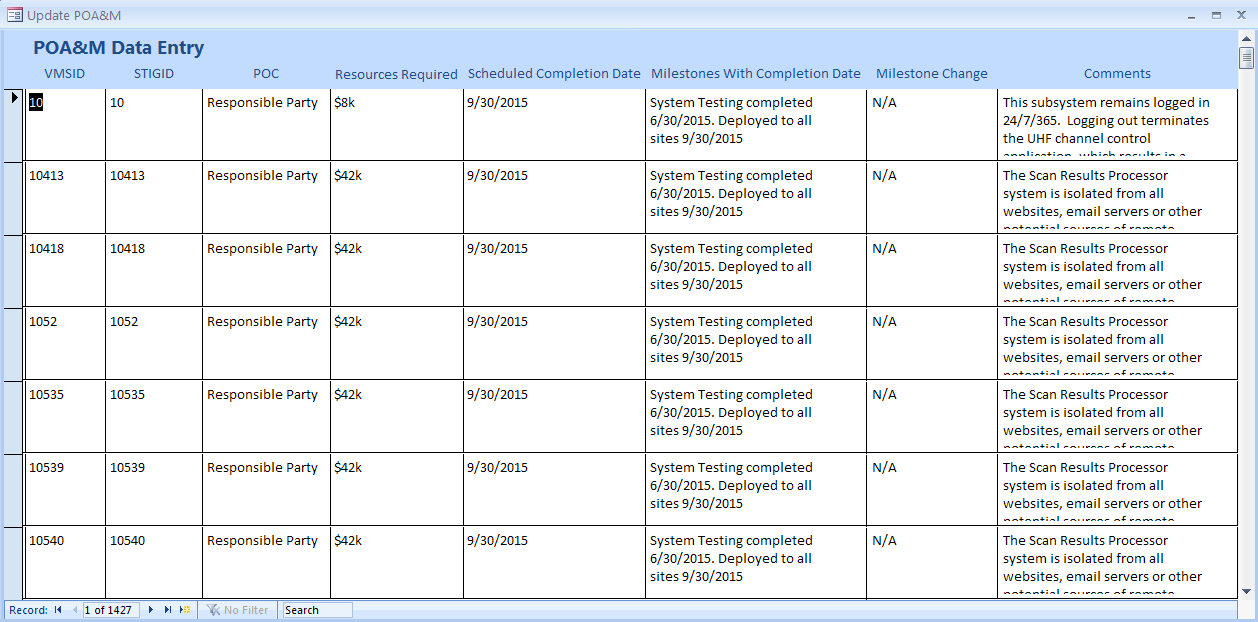
## Plan of Actions and Milestones (POA&M)

The POA&M can be opened by clicking the **Plan of Action & Milestones** button on the MainGui.



**Example of the POA&M**

In addition, the POA&M can be updated with any new vulnerability by clicking the **Update POA&M** button on the MainGui.



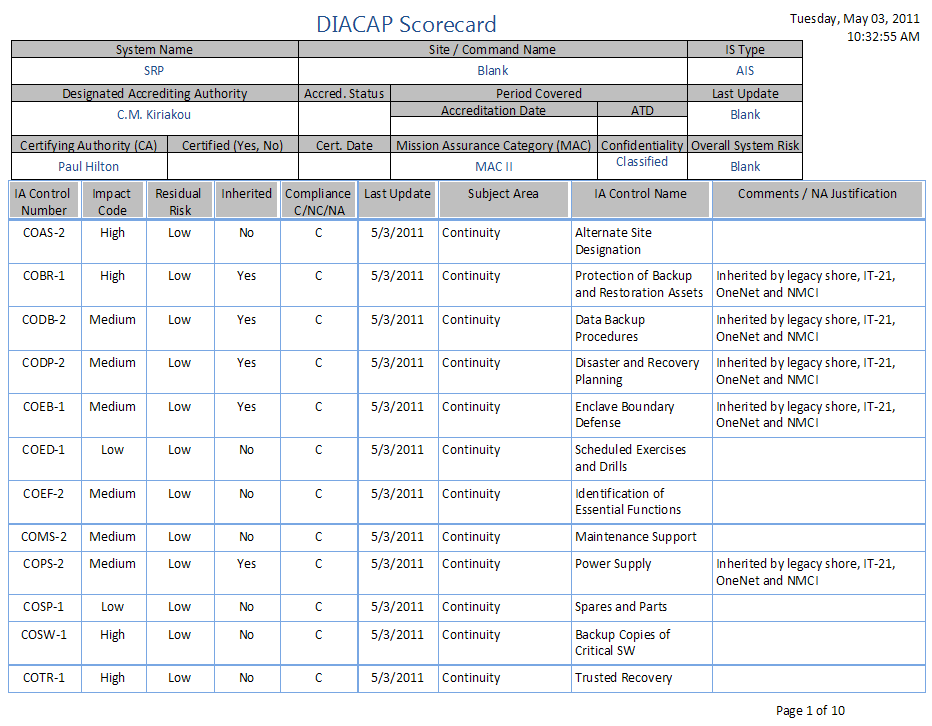
**Example of the Update POA&M page**

The POA&M is opened in Report View in MS Access rather than the normal Print Preview. This allows the user to scroll through findings and export the results to an Excel Spreadsheet. The user can, of course, print this report by clicking **Print**. Understand that this is the full list of all vulnerabilities in the system, Open, Closed and N/A.

Because MS Access tends to truncate data to 255 characters per field, an export to Excel capability has been added to the SRP. A POAM.xlsx file has been included with the SRP. It is pre-formatted and must exist in the same folder as the front end database. Click **Export POA&M to Excel** and the POA&M will be exported. The POA&M.xlsx file is then opened to a tab labeled “qry\_POAM\_Export”. Changes can be made to the format of this document and it will stay formatted for the next export. Just make sure not to rename the tab or to delete the POAM Range. It is always a good idea to copy exports to a different folder. It is recommended to delete all the data on the form before each export as data will overwrite cells, not delete and then write. If you had 1000 lines of data saved in the POAM.xlsx file and then exported again with 500 items, there will still be 1000 items in the spreadsheet.

## DIACAP Scorecard

The DIACAP Scorecard can be opened by clicking the **DIACAP Scorecard** button from the MainGui.

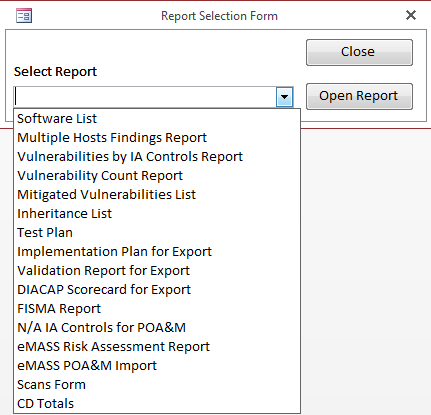


**Example of the DIACAP Scorecard**

The DIACAP Scorecard will show NC or Not Compliant for any IAC associated with an IAC Procedure on the Validation Report that has text in the Vulnerability field. For N/A or Not Applicable IAC, text from the Not Applicable Justification field will be put into the Comments field. For any IAC that is Inherited, text from the Inherited From field will be put into the Comments field. Any NC IAC will include text from the Applied Mitigation field in the Comments.

## Forms & Reports

The Forms & Reports button brings up the Report Selection Form.

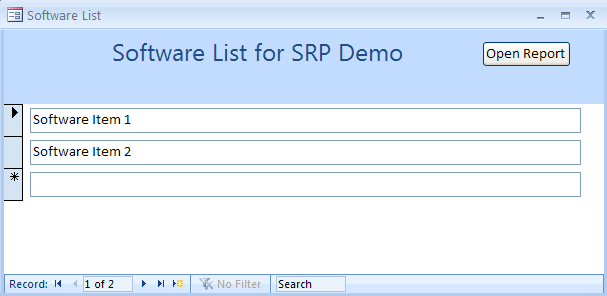


**Example of the Report Selection Form for viewing forms and reports**

To view a form or report, select from the drop down box and click the Open Report button.

### Software List

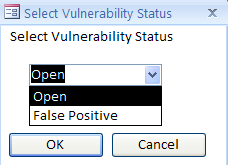
The Software List allows the user to add software items in a form. Anytime a Gold Disk scan is imported, the list of software from the import will automatically be added to the list. A Software List report can be viewed by clicking the Open Report button.



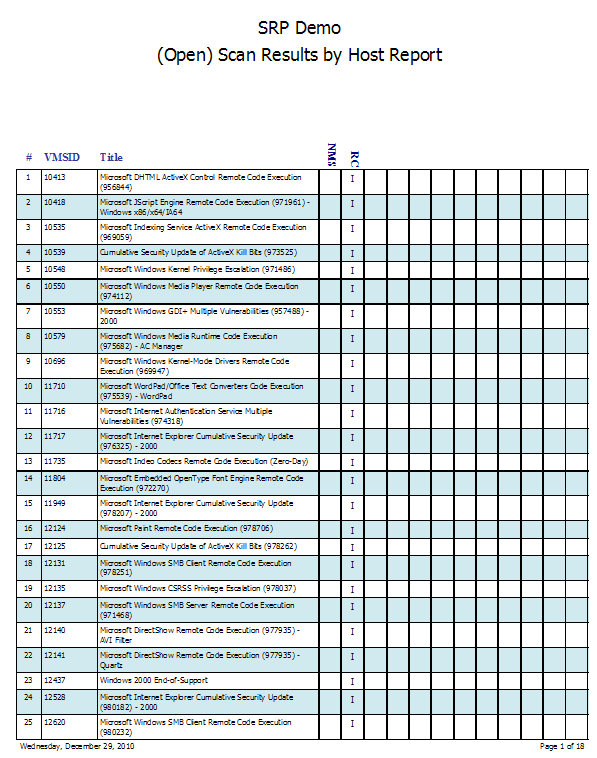
**Example of the Software List Form**

### Multiple Hosts Findings Report

The **Multiple Hosts Findings** **Report** creates a report that displays vulnerabilities grouped as Open, All Open, False Positive, Mitigated, Inherited, etc. The drop down menu allows for selections based on vulnerability status.



**Example of the Select Vulnerability Status dialog box for Multiple Hosts Findings Report**



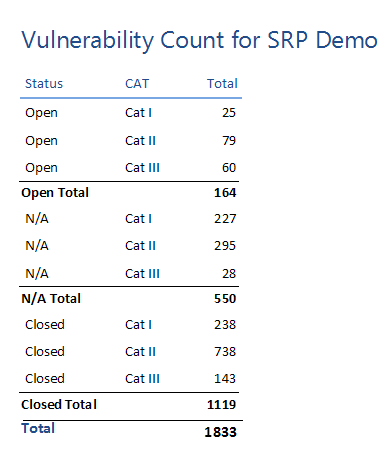
**Example of the** **Multiple Hosts Findings** **Report**

### Vulnerabilities by IA Controls Report

The Vulnerabilities by IA Controls Report provides a list of Vulnerabilities associated with IA Controls and Hosts. Open, Closed and N/A vulnerabilities can be selected.

### Vulnerability Count Report

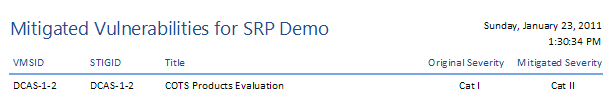
The Vulnerability Count Report is a count of vulnerabilities grouped by status and severity.



**Example of the Vulnerability Count Report**

### Mitigated Vulnerabilities List

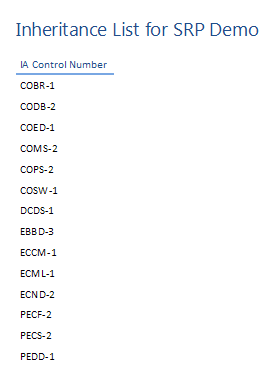
The the Mitigated Vulnerabilities List shows all vulnerabilities that have a different severity from their original severity.



**Example of the POA&M Mitigated Vulnerabilities List**

### Inheritance List

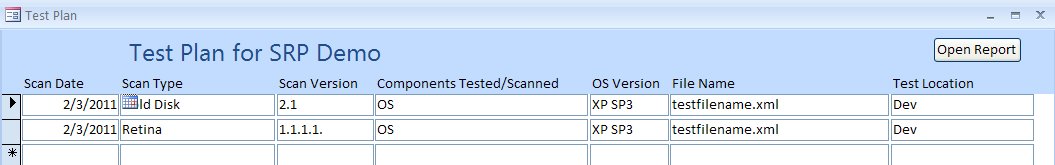
The Inheritance List button will open a list of inherited IA Controls.



**Example of the Inheritance List**

### Test Plan

The Test Plan allows the user to enter the tests (Gold Disk, Retina, SRR, STIGs) run.



**Example of the Test Plan**

Clicking the Open Report button will give a report view of the Test Plan.

### Implementation Plan for Export

The Implementation Plan for Export gives a view of the Implementation Plan suitable for copy paste functionality into a spreadsheet template. In order to prevent truncation of data due to Excel’s paste limitation of 255 characters, with the export query open, select External Data from the Menu, then click the Excel icon from the Export section. Select a file name and location for your new Excel file. Check the <Export data with formatting and layout> check box. Also check the <Open the destination file after the export operation is complete> check box. Click OK. Optionally, you can select the <Export only the selected records> if you selected record in the query.

### Validation Report for Export

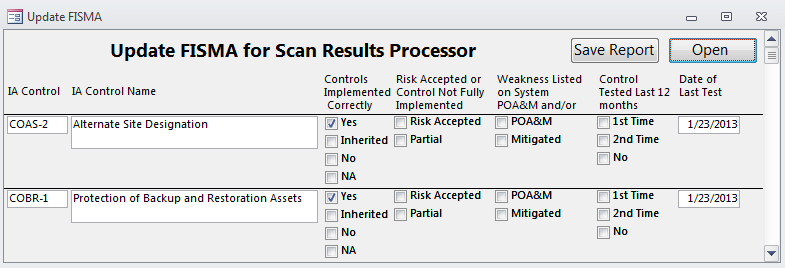
The Validation Report for Export gives a view of the Validation Report suitable for copy paste functionality into a spreadsheet template. In order to prevent truncation of data due to Excel’s paste limitation of 255 characters, with the export query open, select External Data from the Menu, then click the Excel icon from the Export section. Select a file name and location for your new Excel file. Check the <Export data with formatting and layout> check box. Also check the <Open the destination file after the export operation is complete> check box. Click OK. Optionally, you can select the <Export only the selected records> if you selected record in the query.

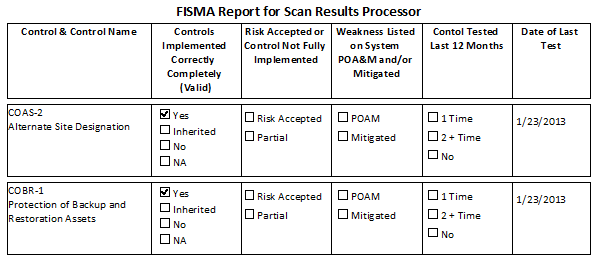
### DIACAP Scorecard for Export

The DIACAP Scorecard for Export gives a view of the DIACAP Scorecard suitable for copy paste functionality into a spreadsheet template. In order to prevent truncation of data due to Excel’s paste limitation of 255 characters, with the export query open, select External Data from the Menu, then click the Excel icon from the Export section. Select a file name and location for your new Excel file. Check the <Export data with formatting and layout> check box. Also check the <Open the destination file after the export operation is complete> check box. Click OK. Optionally, you can select the <Export only the selected records> if you selected record in the query.

### FISMA Report

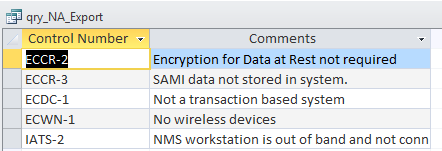
The FISMA Report is used to track the compliance of IA Controls for the First Annual and Second Annual Security Review. Based on test results in the database, some of the fields will be already filled out. Other fields will need to be filled in manually, such as 1st Time and 2nd Time. Clicking the Open button will produce a report that can be reviewed and exported. Clicking the Save Report button will produce a PDF report.





### N/A IA Controls for POA&M

The N/A IA Controls for POA&M query provides a list of the N/A IA Controls that can be used as a reference for entering data into eMASS.



### eMASS Risk Assessment Report

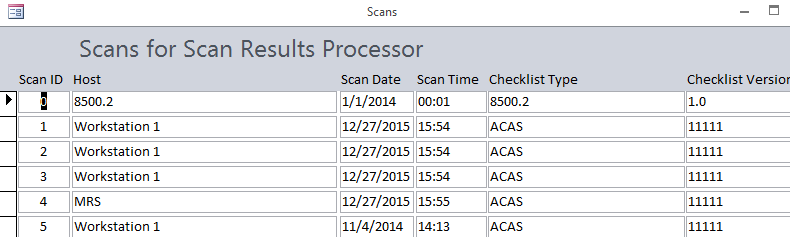
The eMASS Risk Assessment Report creates a query that produces the data required for the eMASS Risk Assessment Report. It has the required data and is in the expected sort order for copying into an eMASS Risk Assessment Report template. After opening the query, select External Data 🡪 Export 🡪 Excel. In the Export window click the Export data with formatting and layout and the Open the destination file after the export operation is complete check boxes. Click Ok. A spreadsheet will open that will allow you to copy and paste into the eMASS Risk Assessment Report template.

### eMASS POA&M Import

The eMASS POA&M Import creates a query that produces the data required for the eMASS POA&M Import. It has the required data and is in the expected sort order for copying into an eMASS POA&M Import template. After opening the query, select External Data 🡪 Export 🡪 Excel. In the Export window click the Export data with formatting and layout and the Open the destination file after the export operation is complete check boxes. Click Ok. A spreadsheet will open that will allow you to copy and paste into the eMASS POA&M Import template. Although the eMASS POA&M Import allows for multiple milestones, the export from Scan Results Processor only allows one milestone per record; one line for each record.

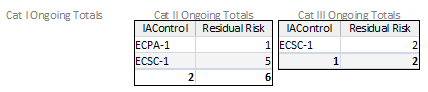
### Scans Form

The Scans form creates a form with a list of all the scans imported into the database.



### CD Totals

The CD Totals creates a report showing the number of findings along with the number of related IA Controls to be used in section 4 of the Certification Determination (CD).



# Troubleshooting

* Verify data is correct, as in importing data.
* Compact and Repair database routinely. Compact the back end database separately from the front end database only when the front end database is closed.
* In order to prevent problems, make sure that when you change data, you click on or go to another record before attempting to close a form or click any buttons.

# Points of Contact

Technical Point of Contact:

Robert Sakey

858-826-9243

robert.m.sakey@saic.com

# Revision History

The Revision History is a list of the changes made to each successive version of the Scan Results Processor. This manual is updated for each version.

## 1.00

* Initial Version

## 1.01

* Split Database into Front End and Back End
* Zipped files into .exe for easier install

## 1.02

* Created choice of Open or False Positive for Multiple Hosts Findings Report
* Inherited From, Not Applicable and Not Applicable Justification is updated on Validation Plan if changed on Implementation Plan
* Added Impact Code from Implementation Plan onto Validation Report
* Fixed bug with Severity being deleted from Validation Report
* Changed Risk Assessment on Validation Report to combo box with values of High, Medium and Low
* Change Severity on Validation Report to combo box with values of Cat I, Cat II and Cat III
* Changed IAC Aggregate Severity on Validation Report to combo box with values of Cat I, Cat II and Cat III
* Fixed bug with Residual Risk not updating Scorecard
* Added an Introduction, Purpose and Scope to this manual
* Added an All Hosts Update box on the Scan Results Form
* Added an Update POA&M button on the main screen GUI that opens a form for entering POA&M data
* Fixes made to ManualScansTemplate.xlsx

## 1.03

* Added “Low” to Residual Risk column on DIACAP Scorecard for all compliant, not applicable and inherited IA Controls
* Modified mouse over text on MainGui
* Increased size of MilestoneChange field in tbl\_UniqueScanResults to 150 characters
* Increased size of IAControl field in tbl\_ManualScans to 100 characters
* Added Hourglass to closure of Scan Results form
* Trapped error when opening front end database with a missing back end database by opening Linked Table Manager
* Added FinalStatus field and changed sort order for POA&M Update form
* Modified Retina import to use sevCode rather than Risk for Severity
* Added tbl\_8500\_Start to back end database in order to create 8500.2 host with ScanID of 0
* Added qry\_8500\_Start in order to create 8500.2 host with ScanID of 0 in tbl\_Scans – record created in tbl\_Scans when database is cleared
* Fixed bug with IAControls not importing correctly for Manual Scans
* Added Add as Vulnerability to Scan Results button to Validation Report Form in order to add 8500.2 Validation Procedures as vulnerabilities, which can be managed from the Scan Results form
* Added additional indexes to various tables to improve query optimization
* Modified code for Scan Results form to propagate changes to other hosts if changes are made to a vulnerability and the AllHosts checkbox is checked
* Modified code to mark Retina vulnerabilities as Closed if they don’t exist on current import and Host names match

## 1.04

* Fixed problem with hourglass on Validation Report
* Fixed problem with single and double quotes in Plan Resolution field in Scan Results Form
* Added tbl\_Software, frm\_Software, rpt\_Software and queries in order to track software from Gold Disk scan and from manual entries on form (changes made to back end database)
* Added Vulnerability Count button to POA&M that opens Vulnerability Count Report
* Added Mitigated Vulnerabilities button to POA&M that opens Mitigated Vulnerabilities List
* Added Inheritance List button to Implementation Plan that opens Inheritance List
* Added tbl\_Color, columns Color (text – 20), ColorValue (long) to tbl\_Defaults and a drop down box on the Setup form to allow the user to select a back color for the MainGui form (changes made to back end database)

## 1.05

* Added Comments field to tbl\_ImplementationPlan, qry\_ImplementationPlan and Implementation Plan form
* Added qry\_ImplementationPlan\_Export to create content to fill Implementation Plan in Navy C&A template
* Added qry\_Scorecard\_Export to create content to fill DIACAP Scorecard in Navy C&A template
* Added frm\_ReportSelection and put a Reports button link to it on the MainGui
* Added tbl\_ReportSelection and qry\_ReportSelection to feed the list of reports on the MainGui
* Removed Software List, Multiple Hosts Findings Report and Vulnerabilities by IA Controls buttons from MainGui
* Increased size of InheritedFrom field in tbl\_ImplementationPlan to 255 characters
* Added tbl\_TestPlan, qry\_TestPlan, frm\_TestPlan, rpt\_TestPlan for Test Plan as required in Navy C&A template
* Prefaced Actual Results in Validation Report Export with Compliant, Non-Compliant, N/A or Inherited
* Added POAMRecommendation, Raw Risk, Likelihood of Exploitation, Magnitude of Impact, Mitigation Effect and Residual Risk fields to tbl\_ValidationPlan, Validation Report and Validation Report Export – all concatenated to create Risk Analysis field in query
* Added tbl\_Software, tbl\_TestPlan and new fields in tbl\_ValidationPlan to delete script when clearing database
* Added POAMFixDate and POAMStatus fields to tbl\_UniqueScanResults and POA&M Update forms to add Completed Date / Risk Accepted Date and Status to POA&M
* Changed Status field on POA&M to “Completed”, “Ongoing”, “Request ODAA to Accept Risk” and “Risk Accepted” along with the date of completion or date of risk acceptance

## 1.06

* Changed Host Selection on MainGui to differentiate between Checklist Types
* Added qry\_Update\_UNIXSource to change Checklist Type for UNIX imports to “UNIX SRR”
* Added ChecklistType and ChecklistVersion fields to tbl\_Scans
* Imports add ChecklistType and ChecklistVersion to tbl\_Scans
* Add Vulnerability to Scan Results button is now invisible if record has already been added to Scan Results preventing same vulnerability being added multiple times
* Added queries qry\_Retina\_AllHosts\_Others, qry\_Retina\_AllHosts\_Update\_AllHosts and qry\_Retina\_AllHosts\_Update\_Status in order to mark closed Retina vulnerabilities automatically when a new Retina scan is imported (effectively, if a Retina vulnerability, that is open for a previous scan for a host, is not found on a new Retina scan, it will mark the vulnerability as closed and if it is found on the new import, it will uncheck the AllHosts checkbox)
* Created MakeTable query, qry\_MakeTable\_Retina\_AllHosts which lists other Retina scans that match the host for the current Retina import; this table is used to update the status of closed Retina vulnerabilities
* Now label colors on MainGui will alternate between black, white or blue based on background color

## 2.00

* Added Splash Screen
* Added qry\_Append\_tbl\_Scans\_UNIXSRR to add “UNIX SRR” as Checklist Type for UNIX imports to tbl\_Scans
* Added ubeVersion field to tbl\_Defaults to allow automatic updates of back end database
* Added table ubeUpdate, forms ubeForm and ubeUpdating and module ubeUpdateCode to database to enable back end updating
* Add Raw Risk to Comments field in POA&M
* Changed Comments field in tbl\_POAM to Memo
* Linked to tbl\_POAM from front end
* Fixed truncation problem with Comments field in POA&M
* Changed size of Plan field in tbl\_ScanResults and tbl\_UniqueScanResults to 27 characters
* Updated Plan checkboxes and drop down box on Scan Results form to include “Request ODAA to Accept Risk”, “Risk Accepted” and “Inherited”
* POAMStatus and POAMFixDate in tbl\_UniqueScanResults automatically update based on values of Plan and PlanStatus on Scan Results Form
* Added Checklist Type and Checklist Version to Scan Results Summary Form and Scan Results Summary Report
* Removed inherited vulnerabilities from showing up on the Validation Report and DIACAP Scorecard
* Added installer

## 2.0.1

* Limited import of Retina vulnerabilities to those that do not have a risk of “information”
* Fixed problem with current results not showing in Scan Summary form
* Fixed problem with Cancel button on Multiple Hosts Selection form not going back to Report Selection form
* Changed Multiple Hosts Findings Report and qry\_Vulnerabilities by adding more selections to Report Type: Inherited, N/A, etc.
* Added qry\_Update\_tbl\_UniqueScanResults\_Null to make sure that there are no null values in the POAMStatus field prior to running the Multiple Hosts Findings Report

## 2.0.2

* Fixed problem with selecting Mitigate in Multiple Hosts Findings Report
* Removed Inherited Vulnerabilities from Validation Report and DIACAP Scorecard
* Fixed Software Report to return to Software Form when closing
* Fixed Test Plan Report to return to Test Plan Form when closing
* Split Inherited vulnerabilities into Inherited – Compliant and Inherited – Ongoing
* Added qry\_Update\_tbl\_ScanResults\_Inherited and qry\_Update\_tbl\_UniqueScanResults\_Inherited to import code to mark closed findings as Inherited – Completed if they are associated with an inherited IA Control

## 2.0.3

* Removed Cat IV vulnerabilities from Update POA&M form
* Changed sort of POA&M to first 53 characters of Source field
* Added qry\_FISMA, frm\_FISMA, rpt\_FISMA and several FISMA fields to tbl\_ImplementationPlan for FISMA compliance report

## 2.0.4

* Change Browse selection on Import Location form to limit to xml or xls based on type of import
* Add ability to import all files from a single folder on Import Location form (or not)

## 2.0.5

* Fixed Add Vulnerabilities button on Validation Report to also delete Vulnerability and Severity from tbl\_ValidationPlan allowing the removal of vulnerabilities from Validation Report when they are Closed
* Filtered FinalStatus in qry\_MitigatedSeverity to only include Open vulnerabilities so Mitigated Vulnerabilities List will only show Open vulnerabilities
* Changed fonts on various forms from MS Sans Serif to Segoe UI
* Changed POAMFixDate field format in tbl\_UniqueScanResults to Short Date so time will not appear on POA&M in Status column
* Removed Plan options of Request ODAA to Accept Risk and Risk Accepted from Scan Results Form
* Increased height of Plan combo box on Scan Results Form
* Added cmdClose field to tbl\_Defaults to account for the need to run code if changes were not made to the Scan Results Form
* Set default of 0 to cmdClose when opening Scan Results Form
* Changed cmdClose to 1 when changes are made to Scan Results Form
* Code run on close of Scan Results Form will now only run if changes are made to Plan, Plan Status, All Hosts or IA Controls
* Added code to check if a Gold Disk vulnerability, that is open for a previous scan for a host, is not found on a new Gold Disk scan, then it will mark the vulnerability as closed
* Added code to change POAM Status to Completed and add a POAM Completed Date when a vulnerability from an imported Retina or Gold Disk scan is no longer Open

## 2.0.6

* Scan Date and Scan Time are prepopulated with Import File Date/Time stamp for all file imports
* Added ability to change Host name on Update Scan Date & Scan Time form for Gold Disk and Retina Imports
* Added ability to import VMS Export files – these files are created by the DISA STIG Viewer
* When creating VMS Export files, the user must set the Severity Override or no Severity will be imported
* Increased size of Hosts field in tbl\_Hosts from 50 to 255 because it was being truncated with multiple hosts in the POA&M Source column
* Fixed Validation Report erasing data for procedures not ending in “-1”
* Fixed Validation Report erasing Applied Mitigation for procedures ending in “-1”
* Fixed Validation Report using Severity instead of OrigSeverity for Raw Risk when creating a vulnerability from an 8500.2 procedure
* Adjusted query for creating initial 8500.2 Scan by adding Checklist Type and Checklist Version
* Changed Status field on POA&M to not include time
* Added ECID-1 to MAC III IA Controls
* Fixed Yes and No showing up as TRUE and FALSE on Implementation Plan Export
* Fixed mitigated vulnerabilities not filtering correctly when using the Severity filters
* Updated Validation Report to use IAC Impact Code as Original Severity when creating a vulnerability from an 8500.2 procedure; High = Cat I, Medium = Cat II and Low = Cat III
* Added ability to view Manual Fix from Scan Results Form by double clicking Discussion field
* Added Manual Fix to Scan Results Report
* Added Checklist Type to Scan Results Form
* Limit of 38 vulnerabilities added to any one IA Control in Validation Report due to error message

## 2.0.7

* Handled double quotes in vulnerability field in Validation Report

## 2.0.8

* Changed query for updating vulnerabilities on Validation Report to not add vulnerabilities to N/A IA Controls
* Added button to POA&M to make two different exports, one with N/A vulnerabilities and one without N/A vulnerabilities for Navy ODAA templates (individual N/A vulnerabilities should not be put onto POA&M
* Added qry\_NA\_Export to Report Selection Form to allow export for N/A IA Controls on Navy ODAA POA&M Template
* Added Select check box and Update Select check box to Scan Results Form (functionality to be used later)
* Fixed invalid use of null error on Scan Results Form caused by first entering data into the Plan Resolution field, deleting the entire contents of the Plan Resolution field, then going to the next record
* Made All Hosts checkbox on Scan Results Form checked by default on scan import

## 2.0.9

* Created tbl\_ScanResults\_Update Comments to allow automatic update of N/A, Closed and Mitigation comments
* Updated qry\_Update\_tbl\_ScanResults\_Inherited and qry\_Update\_tbl\_UniqueScanResults\_Inherited by adding qry\_Update\_tbl\_ScanResults\_Inherited1 to limit the selection of vulnerabilities to those that are uniquely associated with inherited IA Controls
* Created tbl\_STIGViewer, qry\_Append\_STIGViewer, qry\_Append\_tbl\_Scans\_STIGViewer and added STIG Viewer Import option to Import Data to allow the import of STIG Viewer CSV file

## 3.0.0

* Created qry\_RiskAssessment and eMASS Risk Assessment form for new artifact required to be uploaded to eMASS
* Created frm\_Additional Comments, accessible from Scan Results form by double clicking Resolution field, in order to account for additional comments required by eMASS Risk Assessment form
* Added MitigationDescription, RemediationDescription, RiskAssessment and CorrectiveAction fields to tbl\_ScanResults and tbl\_UniqueScanResults
* Increased size of IAControl field in tbl\_ManualScans to 30

## 3.0.1

* Created qry\_eMASS\_POAMImport in order to upload weakness to eMASS for use with eMASS POA&M Import Template
* Added eMASS POA&M Import Report to list of reports
* Changed font of Date field in Scan Results Report from 78 to 8
* Added qry\_Hosts\_Open, qry\_Hosts\_Closed and qry\_Hosts\_Closed Without Matching qry\_Hosts\_Open along with a change in code for the Scan Results Form and when importing scans that will change the Source Identifying Weakness to show, for Open vulnerabilities, only those Hosts for which the vulnerability is Open. For vulnerabilities that are Open, Closed or N/A for all Hosts, the Source Identifying Weakness will show all Hosts
* Changed Manual Scan import to use date/time from data in spreadsheet vice file date/time on Update Scan Date/Time form
* Ignore error 3624 when using Replace All functionality on Scan Results Form when cursor is not in first record
* Change behavior of all imports to mimic Retina import in that if a previous item for that Host was Open and a new scan shows it as closed, the POAMStatus will change to “Completed”

## 3.0.2

* Fixed problem where a new scan with an Open vulnerability was not changing the POAM Status to Ongoing from Completed if the vulnerability is Open for a different Host
* Using Update Selected Data form from Scan Results Form now updates POA&M Status and POA&M Fix Date
* Managed error when opening front end database with no linked back end database
* Added combo box to Host field on Update Scan Date and Time form to allow for selecting already existing host name
* Removed “Retina Audit ID” text from 8500.2 findings in eMASSPOAMImport
* Changed default report type to “All Open” on Multiple Hosts Findings Report
* Added LOE data to Likelihood column in eMASS Risk Assessment Report
* Removed references to Gold Disk in Defaults form, tables and queries
* Added query and form, frm\_Scans, to allow for changing Scan/Host information
* Double clicking Mitigation Description or Remediation Description labels on Additional Comment form enters stock data
* Added Navigation buttons to FISMA form
* Set default database directory to current project path
* Added Refresh Table Links code to Public Module to automatically link to a back end database in the same directory as the front end database if existing link is broken
* Changed qry\_Hosts\_Closed to look for FinalStatus = Closed instead of Status = Closed

## 3.0.3

* Fixed problem with quotes in Mitigation Description field on Scan Results form
* Right justify Scan Time field on Update Scan Date & Time form
* Now adding Date/Time and Resolution when creating vulnerabilities from Validation Report
* Added text to bottom of Validation Report noting that vulnerability has been added
* Added combo boxes to Checklist Type and Checklist Version on Import Location form
* Set Font Color to red on IA Control tab if no IA Control is associated with Vulnerability on Scan Results form
* Updated cve field in audit table to Memo
* Updated Comments, CCI Data and False Positive fields in tbl\_STIGViewer to Memo
* Changed code on Scan Results form to replace double quotes with single quotes in Resolution field
* Removed Vulnerator with ACAS as a choice of Import Type
* Added code, tables and queries to support ACAS imports: tbl\_ACAS, qry\_Update\_ACAS, qry\_Append\_ACAS, qry\_Append\_tbl\_Scans\_ACAS, qry\_Update\_ACAS\_Import\_Old\_Findings, qry\_ACAS\_Import, qry\_Update\_POAM\_Old\_Findings\_ACAS, qry\_MakeTable\_ACAS\_AllHosts, qry\_ACAS\_AllHosts\_Others, qry\_ACAS\_AllHosts\_Others\_Update\_AllHosts, qry\_ACAS\_AllHosts\_Others\_Update\_Status

## 3.0.4

* Time and Date now updates on Scan Results form for previously Open Retina or ACAS findings when a new scan is imported with that finding Closed
* POAM Fix Date now updates to blank when using Update Selected Data form and updating Plan Status to Not Done.
* Plan Status now updates correctly in tbl\_UniqueScanResults when using Update Selected Data form and updating Plan Status.
* Final Status now updates correctly in tbl\_ScanResults and tbl\_UniqueScanResults when using Update Selected Data form and updating Plan Status.
* Fixed inability to check Selected check box after sorting by a header
* Removed hourglass on error on closing Scan Results form
* Added pop-up in addition to hourglass when importing scan
* Minor changes made to Validation Report form to conform to Validation Report export requirements
* Updated Checklist field on Scan Results form to include Checklist Version
* Added CD Report and queries to show the count of Cat I, Cat II and Cat II findings and IA Controls for Ongoing findings listed on the RAR
* Added a button on the MainGui to filter scans for either All Scans or Latest Scans
* Updated IA Control button on Scan Results form to also show blue text for associated IA Controls that are N/A

## 4.0.0

* Fixed issue with opening 8500.2 scan results
* Added Back End database backup button
* Added Compact on Exit button
* Added button to select only the latest scans for a host
* Changed tbl\_STIGViewer Severity Override Guidance, Rule Title, False Negatives and CCI Data from Short Text to Long Text
* Updated Checklist Version for 8500.2 scan to MAC / CL
* Updated POA&M Import, RAR and POA&M to use Checklist Type and Checklist Version from tbl\_Scans
* Default for Scan Imports is now STIG Viewer
* Updated ACAS Scan Imports to require Checklist Version (Plugin ID)
* Removed UNIX Scans and Retina Scans from Import Location Form
* Moved code to concatenate IA Controls for each vulnerability to closing IA Control subform from closing Scan Results Form
* Moved code to concatenate Hosts for source of vulnerability to changes to Plan and PlanStatus on Scan Results Form
* Added message box on Import Location Form to pop up when the Import Location field is blank
* Notification on Scan Results form when closing scan form if any No Plan Yets remain
* Add Vulnerability to Scans button on Validation Report has been removed if procedure has already been added to scans
* Fixed error message when adding a validation procedure as a vulnerability without setting the Severity
* Changed code when changing PlanStatus to correctly mark same vulnerability for other scans whether All Hosts checkbox is checked or not
* Updated Scan Results Form to display a message and then close if there are no records
* Fixed code on Update Selected Records form to correctly mark Final Status, hosts and resolution for all scans
* Added button on Setup screen to update VMSID/IA Control links, which are built from associating IA Controls with vulnerabilities
* Added combo box to Setup screen to turn paint on/off for the IA Control button on the Scan Results form
* Text color of IA Control button changes based on underlying value: black if one or more IA Controls exist, red if no IA Controls exist and blue if the IA Control is marked as N/A
* Fixed problem with importing back to back scans
* Added ability to import scans from ACAS SecurityCenter in addition to ACAS Nessus, using the Detailed Vulnerability Report provided by DISA
* Added Host Name to Import Location form for ACAS scans

## 4.0.1

* Fixed issue with changes to Plan and Plan Status causing a refresh of the Scan Results form
* Fixed issue with changes to Select checkbox causing a refresh of the Scan Results form
* Fixed issue with No Plan Yet dialog box appearing when closing form and No records have No Plan Yet as a Plan status
* Removed inherited findings from POAM
* Removed warning if Plan is Inherited – Ongoing and Plan Status is Not Done

## 4.0.2

* All imports now create and then delete a temp copy of import file just in case file name is longer than Microsoft Access limit of 64 characters
* On Import Location form, blank fields will pop up a message back
* Change choice of file extension for Importing ACAS Nessus, ACAS SecurityCenter and STIG scans to \*.csv only
* Added Host sorting on MainGui
* Added automatic Checklist Version selection based on Checklist Type on Import Location form
* Automatically create temp file when importing to remove problem with file name being too large
* Changed progress form when importing scans
* Removed code that updated Scan Results table when Title, Description and Discussion fields are changed
* Added code after update of Title, Description and Discussion fields to change these fields for all instances of the changed finding
* Updated query to allow changes to Manual Fix field in Unique Scans table
* Double clicking VMSID in Scan Results Form pops up sub form with all findings with matching VMSID
* Added button to display Missing IA Controls on Scan Results Form
* Added RuleID field to tbl\_ManualScans, tbl\_ScanResults and tbl\_UniqueScanResults
* Updated eMASS POA&M Import with changed header names based on eMASS v.5.3
* Added Security Checks, Mitigations and Raw Severity Value to eMASS POA&M Import v5.3

## 4.0.3

* Added sorting by Scan ID for Scan Results
* MainGui is now visible if Import Location Form is closed
* Importing Closed findings when earlier scans are marked as N/A now mark it as N/A
* Added “Info” results to ACAS scans as Cat IV findings, which do not appear on Scan Results Form
* Adjusted width of ScanID field on Scan Summary form and report
* Added error handling to Scan Results form if attempting to close an empty recordset (8500.2 with no results)

## 4.0.4

* Added All Scan Results Form
* Added H, M and L buttons on Additional Comments form
* Added Dollar amount buttons on Update POA&M form

## 4.0.5

* Changed size of Scan Results Form
* Added Clear button to Update POA&M form
* Added Missing IA Controls button to show query of missing IA Controls on Scan Results Form and All Scan Results Form
* Updated format of Scan Results Report and All Scan Results Report
* Added IA Control Paint feature to Scan Results Form and All Scan Results Form
* Added green text to IA Control button on Scan Results Form and All Scan Results Form to denote Inherited IA Controls
* Changed size of All Scan Results Form
* Added All Open Scan Results Report to All Scan Results Form to show all open findings in database
* Added Mismatched Results button to show query of Mismatched Results on All Scan Results Form
* Fixed bugs on All Scan Results Form
* Removed Update ‘All Hosts’ (All) checkbox from Scan Results Form
* Changed Backend Backup icon on MainGui to button stating Backend Backup
* Added Select Database button to MainGui to allow user to select any Backend Database – promoting the use of one front end for many back end databases
* Added text string at top of MainGui showing location of back end database
* Updated Source Identifying Weakness field on POA&M to show each Host/Checklist Type/Checklist Version for Open findings
* Modified query and selection for Multiple Hosts Findings Report to fix bugs
* Removed existing Software Table
* Added Software List Table, Query, Form and Report to match Software List table in C&A Plan
* Added Hardware List Table, Query, Form and Report to match Hardware List table in C&A Plan
* Added PPS Table, Query, Form and Report to match PPS table in C&A Plan
* Updated Vulnerabilities by IA Controls Report by removing Host and Status and linking to tbl\_UniqueScanResults vice tbl\_ScanResults

## 4.0.6

* Added ability to update STIGID on Scan Results Forms
* Added Check Content and Discussion to Manual Fix subform
* More Information subform opens when double clicking Description instead of Discussion
* Discussion field has been removed from Scan Results Form and All Scan Results Form
* Added STIG Comments to More Information subform
* Updated Resolution with STIG Comments if Resolution is blank
* Updated all subqueries on Scan Results Form and All Scan Results Form to subforms
* All subforms on Scan Results Form and All Scan Results Form close when parent form is closed
* Double clicking VMSID on some subforms goes to that record on parent form

## 4.0.7

* Updated All Scan Results Form code to set ScanToView and FindingToView in tbl\_Defaults
* Updated Level of Effort query to show distinct IA Controls
* Updated query to create Hosts table by removing Checklist Version

## 4.0.8

* Added Latest Scans button to All Scan Results form
* Tweaked spacing on Scan Results Report
* STIG imports no longer create an Import failure table on SeverityOverrideGuidance field being truncated
* Mismatched Results and Missing IA Controls button now refresh after making a change and then re-clicking the buttons on Scan Results and All Scan Results forms
* Severity combo box is disabled unless Plan is set to Mitigate on Scan Results and All Scan Results forms
* Major overhaul of the code for updating tbl\_UniqueScanResults during a scan import, and by changing Plan or Plan Status on Scan Results Form and All Scan Results Form

## 4.0.9

* Added Clear All Data button to Additional Comments form
* Updated sort options for selecting Host on MainGui
* Updated More Information form to pull data from tbl\_ScanResults vice tbl\_UniqueScanResults
* Updated Plan, PlanStatus and Import If-Then flow

## 4.0.10

* Added ability to Baseline Open Findings in addition to several reports based on baseline (for eMASS POAM Import template
* Fixed bug when changing finding to N/A wasn’t setting POAMStatus to N/A

## 4.0.11

* Updated All Scans Open Report to include Checklist Version
* Updated Multiple Host Findings Report to only include latest scans for each host/checklist
* Updated Missing IA Controls form to include Checklist and to sort by header
* Added Baseline Check Box on Additional Comments screen

## 4.0.12

* Fixed Hosts table to add Checklist Type used for Source column of POA&M

## 4.0.13

* Added ability to import from STIG Viewer 2.5.X

## 4.0.14

* Changed Import Location Form to automatically check for the STIG Viewer version

## 4.0.15

* Fixed Navigation Pane opening when importing STIG
* Fixed setting POAMStatus when creating vulnerability from Validation Procedures
* Added CVE field from ACAS SecurityCenter scan to CheckContent