**Scan Results Processor (SRP)**

**USER’S MANUAL**

*Robert Sakey*

RMF Version 1.4.2: August 22, 2018

**Revision Sheet**

|  |  |  |  |
| --- | --- | --- | --- |
| **Release No.** | **Date** | **Revision Description** | **Author** |
| 1.0.0 | 3/5/2017 | Initial Release | Robert Sakey |
| 1.0.1 | 3/14/2017 | Changes to Security Controls and Assessment Procedures | Robert Sakey |
| 1.1.0 | 3/24/2017 | First major production version | Robert Sakey |
| 1.2.0 | 4/04/2017 | Added export buttons for SC and AP forms, added Tier 3 Inheritance, changed Overlay buttons | Robert Sakey |
| 1.2.1 | 4/7/2017 | Changed STIG Viewer Import to automatically test for version | Robert Sakey |
| 1.2.2 | 4/18/2017 | Minor fixes. First use of Back End Updater | Robert Sakey |
| 1.2.3 | 4/19/2017 | Fixes for vulnerabilities field on Assessment Procedures form, ChecklistType changes and ACAS scans with no findings | Robert Sakey |
| 1.2.4 | 4/25/2017 | Fixed Security Controls column on POA&M | Robert Sakey |
| 1.2.5 | 4/27/2017 | General cleanup; minor fixes | Robert Sakey |
| 1.2.6 | 5/3/2017 | Security Controls, Overlay and Back End Backup fixes | Robert Sakey |
| 1.2.7 | 5/9/2017 | Fixed Control values | Robert Sakey |
| 1.3.0 | 5/10/2017 | Added functionality to Assessment Procedures Form | Robert Sakey |
| 1.3.1 | 5/18/2017 | Added functionality to Assessment Procedures Form and Import Location Form | Robert Sakey |
| 1.3.2 | 6/14/2017 | Updated field size in Security Plan; Added version checks; Tier 3 Inheritance added to Assessment Procedures | Robert Sakey |
| 1.3.3 | 8/21/2017 | Fixed major bug in Nessus imports. Other minor changes | Robert Sakey |
| 1.3.4 | 2/15/2018 | Lots and lots of changes, especially to Assessment Procedures and Security Controls forms | Robert Sakey |
| 1.3.5 | 3/27/2018 | Added StatCounter functionality to optionally track IP addresses of users | Robert Sakey |
| 1.3.6 | 4/19/2018 | Added Security Assessment Plan (SAP) | Robert Sakey |
| 1.3.7 | 5/3/2018 | Added Monitored Control Information for Continuous Monitoring Plan | Robert Sakey |
| 1.3.8 | 5/7/2018 | Added Unmonitored Control Information and automated Control Criticality for Continuous Monitoring Plan | Robert Sakey |
| 1.3.9 | 5/17/2018 | Added Last Update field and fixed Continuous Monitoring forms | Robert Sakey |
| 1.3.10 | 5/24/2018 | Updated Continuous Monitoring form and Implementation Plan query. Fix for duplicates on POA&M | Robert Sakey |
| 1.3.11 | 5/30/2018 | Updated Continuous Monitoring form | Robert Sakey |
| 1.3.12 | 5/30/2018 | Code from previous changes was lost and put back along with tweaks to it | Robert Sakey |
| 1.3.13 | 7/10/2018 | Added FISMA Year 1,2 and 3 plus minor fixes and tweaks | Robert Sakey |
| 1.4.0 | 7/11/2018 | Fixed CCI Import and calls to Excel and github.com | Robert Sakey |
| 1.4.1 | 7/24/2018 | Minor fixes, CCI update based on 7/2018 STIG compilation | Robert Sakey |
| 1.4.2 | 8/22/2018 | Major fixes including fields for Risk Assessment | Robert Sakey |

**TABLE OF CONTENTS**

[1 Introduction 7](#_Toc522695847)

[1.1 Purpose 7](#_Toc522695848)

[1.2 Scope 7](#_Toc522695849)

[2 Getting Started 7](#_Toc522695850)

[2.1 System Requirements 7](#_Toc522695851)

[2.2 Scan Results Processor Contents and Description 7](#_Toc522695852)

[2.3 Installation 8](#_Toc522695853)

[2.3.1 Install Scan Results Processor 8](#_Toc522695854)

[2.3.2 Copy SRP to Working Directory 8](#_Toc522695855)

[2.4 Starting the Scan Results Processor 8](#_Toc522695856)

[3 MainGui 10](#_Toc522695857)

[3.1 Back End Databases 10](#_Toc522695858)

[3.2 Setup Form 11](#_Toc522695859)

[3.2.1 Setup data 12](#_Toc522695860)

[3.2.2 Security Controls 12](#_Toc522695861)

[3.2.3 Assessment Procedures 12](#_Toc522695862)

[3.2.4 POA&M 12](#_Toc522695863)

[3.2.5 Form Color 12](#_Toc522695864)

[3.2.6 Procedure Paint On/Off 12](#_Toc522695865)

[3.2.7 AutoBackup 12](#_Toc522695866)

[3.2.8 Control Selection 13](#_Toc522695867)

[3.2.8.1 800-53 Control Selection 13](#_Toc522695868)

[3.2.8.2 Setup Overlays 13](#_Toc522695869)

[3.2.8.3 Open Controls Report 15](#_Toc522695870)

[3.2.8.4 Open Controls Report - Details 15](#_Toc522695871)

[3.2.8.5 Open Controls Report - Procedures 15](#_Toc522695872)

[3.2.8.6 Open IA Controls Report 15](#_Toc522695873)

[3.2.8.7 Open Form 15](#_Toc522695874)

[3.2.8.8 Open Common Controls Report 15](#_Toc522695875)

[3.2.8.9 Remove Additional Controls 15](#_Toc522695876)

[3.2.9 Update CCIs 15](#_Toc522695877)

[3.2.10 Clear Database 16](#_Toc522695878)

[3.2.11 Baseline 16](#_Toc522695879)

[3.2.12 Relink Database 16](#_Toc522695880)

[3.3 Backend Backup 17](#_Toc522695881)

[3.4 Exit 17](#_Toc522695882)

[3.5 Compact Off/On 18](#_Toc522695883)

[3.6 IAVM 18](#_Toc522695884)

[3.6.1 Project Form 18](#_Toc522695885)

[3.6.2 IAVM Forms 18](#_Toc522695886)

[3.6.3 IAVM Reports 19](#_Toc522695887)

[3.6.4 Import IAVMs 20](#_Toc522695888)

[3.7 Security Plan 21](#_Toc522695889)

[3.8 Security Controls 21](#_Toc522695890)

[3.8.1 Monitored Control Information 22](#_Toc522695891)

[3.8.2 Unmonitored Control Information 23](#_Toc522695892)

[3.9 Assessment Procedures 23](#_Toc522695893)

[3.10 Plan of Action & Milestones 24](#_Toc522695894)

[3.11 Update POA&M 25](#_Toc522695895)

[3.12 Scan Summary 25](#_Toc522695896)

[3.13 Scan Results 27](#_Toc522695897)

[3.13.1 Viewing Vulnerabilities 28](#_Toc522695898)

[3.13.2 Updating Vulnerabilities 28](#_Toc522695899)

[3.13.3 Dealing with Vulnerabilities that are Open on one Host and Closed on Another 30](#_Toc522695900)

[3.13.4 Scan Results Report 30](#_Toc522695901)

[3.13.5 Missing Controls 31](#_Toc522695902)

[3.13.6 Procedure Paint On/Off 32](#_Toc522695903)

[3.13.7 Closing the Scan Results Form 32](#_Toc522695904)

[3.14 All Scan Results 32](#_Toc522695905)

[3.14.1 All Scan Results Report 32](#_Toc522695906)

[3.14.2 Click to Show Only Latest Scans 32](#_Toc522695907)

[3.14.3 Missing Controls 33](#_Toc522695908)

[3.15 Import Data 33](#_Toc522695909)

[3.16 Forms & Reports 35](#_Toc522695910)

[3.16.1 Scans Form 36](#_Toc522695911)

[3.16.2 Software List 36](#_Toc522695912)

[3.16.3 Hardware List 37](#_Toc522695913)

[3.16.4 PPS List 37](#_Toc522695914)

[3.16.5 Test Plan 37](#_Toc522695915)

[3.16.6 Inheritance List 37](#_Toc522695916)

[3.16.7 Mitigated Vulnerabilities List 38](#_Toc522695917)

[3.16.8 N/A Security Controls List 39](#_Toc522695918)

[3.16.9 FISMA Report 39](#_Toc522695919)

[3.16.10 All Open Scans Results Report 40](#_Toc522695920)

[3.16.11 Multiple Hosts Findings Report 40](#_Toc522695921)

[3.16.12 Vulnerabilities by Security Controls Report 42](#_Toc522695922)

[3.16.13 Vulnerability Count Report 42](#_Toc522695923)

[3.16.14 Vulnerability Count Report per Checklist 44](#_Toc522695924)

[3.16.15 Vulnerability Count Report per Checklist – No Severity 45](#_Toc522695925)

[3.16.16 eMASS Risk Assessment Report (RAR) 46](#_Toc522695926)

[3.16.17 eMASS POA&M Import (All Ongoing Findings) 46](#_Toc522695927)

[3.16.18 eMASS POA&M Import (Baselined Ongoing Findings) 46](#_Toc522695928)

[3.16.19 eMASS POA&M Import (New Findings Since Baseline) 46](#_Toc522695929)

[3.16.20 eMASS POA&M Import (Closed Findings Since Baseline) 46](#_Toc522695930)

[3.16.21 eMASS Test Result Import 46](#_Toc522695931)

[3.16.22 eMASS Implementation Plan (Assigned Security Controls) 46](#_Toc522695932)

[3.16.23 eMASS Risk Assessment Summary 46](#_Toc522695933)

[3.16.24 eMASS Security Assessment Report (SAR) Sheet 1 47](#_Toc522695934)

[3.16.25 eMASS Security Assessment Report (SAR) Sheet 2 47](#_Toc522695935)

[3.16.26 CD Totals 47](#_Toc522695936)

[3.16.27 STIG/SRG Selection Form 47](#_Toc522695937)

[3.16.28 Findings with Unselected Controls Report 48](#_Toc522695938)

[3.16.29 Security Assessment Plan 49](#_Toc522695939)

[3.16.29.1 Assessment Architecture – System Name – Section 1.0 50](#_Toc522695940)

[3.16.29.2 Assessment Architecture – Baseline Hardware List – Section 1.1 50](#_Toc522695941)

[3.16.29.3 Assessment Architecture – Baseline Software List – Section 1.2 51](#_Toc522695942)

[3.16.29.4 Assessment Methods – Requirements Traceability – Section 2.1 51](#_Toc522695943)

[3.16.29.5 Assessment Personnel & Schedule – Assessment Personnel – Section 3.1 51](#_Toc522695944)

[3.16.29.6 Assessment Personnel & Schedule – Assessment Schedule – Section 3.2 52](#_Toc522695945)

[3.16.29.7 Exceptions – Exceptions in Testing – Section 4.0 52](#_Toc522695946)

[3.16.29.8 Security Test Report – False Positives – Section 5.1 53](#_Toc522695947)

[3.16.29.9 Security Test Report – Misleading Reports – Section 5.2 54](#_Toc522695948)

[3.16.29.10 Security Test Report – Summary of Issue: Background – Section 5.3 54](#_Toc522695949)

[3.16.29.11 Security Assessment Plan – Export 54](#_Toc522695950)

[4 Troubleshooting 54](#_Toc522695951)

[4.1 Windows 54](#_Toc522695952)

[4.2 Microsoft Office 2007 55](#_Toc522695953)

[4.3 Verify data is correct 55](#_Toc522695954)

[4.4 Compact and Repair 55](#_Toc522695955)

[4.5 Changing Data Issues 56](#_Toc522695956)

[4.6 Database goes to code window when opening for the first time 56](#_Toc522695957)

[4.1 Error Updating Back End Database after installing new version 56](#_Toc522695958)

[5 How to create new build of SRP and post to GitHub 56](#_Toc522695959)

[6 Point of Contact 57](#_Toc522695960)

[7 Revision History 57](#_Toc522695961)

[7.1 1.0.0 57](#_Toc522695962)

[7.2 1.0.1 57](#_Toc522695963)

[7.3 1.1.0 58](#_Toc522695964)

[7.4 1.2.0 58](#_Toc522695965)

[7.5 1.2.1 58](#_Toc522695966)

[7.6 1.2.2 58](#_Toc522695967)

[7.7 1.2.3 59](#_Toc522695968)

[7.8 1.2.4 59](#_Toc522695969)

[7.9 1.2.5 59](#_Toc522695970)

[7.10 1.2.6 59](#_Toc522695971)

[7.11 1.2.7 59](#_Toc522695972)

[7.12 1.3.0 59](#_Toc522695973)

[7.13 1.3.1 60](#_Toc522695974)

[7.14 1.3.2 60](#_Toc522695975)

[7.15 1.3.3 61](#_Toc522695976)

[7.16 1.3.4 61](#_Toc522695977)

[7.17 1.3.5 62](#_Toc522695978)

[7.18 1.3.6 62](#_Toc522695979)

[7.19 1.3.7 62](#_Toc522695980)

[7.20 1.3.8 63](#_Toc522695981)

[7.21 1.3.9 63](#_Toc522695982)

[7.22 1.3.10 63](#_Toc522695983)

[7.23 1.3.11 64](#_Toc522695984)

[7.24 1.3.12 64](#_Toc522695985)

[7.25 1.3.13 64](#_Toc522695986)

[7.26 1.4.0 64](#_Toc522695987)

[7.27 1.4.1 65](#_Toc522695988)

[7.28 1.4.2 65](#_Toc522695989)

# Introduction

The Cybersecurity (CS) community uses numerous tools to test, scan, document, and present an information system’s security posture under the Risk Management Framework (RMF). The Scan Results Processor (SRP) provides an automated means to process, document, and present the raw data captured in the various CS testing, scans, and checklists. SRP provides the processed data in the format and on the forms required in RMF.

## Purpose

This user’s manual 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 RMF process and provides data in established forms and formats.

# Getting Started

## System Requirements

* Microsoft Windows 7, 10
* Microsoft Office 2010 or newer
  + Scan Results Processor database built with Access 2016 and may require work-arounds to work in older versions of Access (see troubleshooting section)
* STIG Viewer (optional)
  + Tool for aggregation of security findings for systems
  + Located on the iase.disa.mil website
  + Currently supports, at a minimum, versions 1.2 through 2.6.1
* ACAS (optional)
  + Tool for scanning Windows, Linux and UNIX computers
  + Located on the iase.disa.mil website
* 200 MB of free hard drive space
  + Capacity to host SRP files as well as scan data
  + Installation requires 30 MB of free hard drive space
  + The back end database starts at 20 MB and can grow considerably after importing scans

## Scan Results Processor Contents and Description

* Scan Results Processor – RMF x.x.x.accdb
  + Front end database file used for importing, processing, and display of scan data.
  + Can be overwritten with new versions
* Scan Results Processor – RMF x.x.x be.accdb
  + Back end database file used for storing scan data.
  + Should not be overwritten with new versions
* POAM.xlsx.
  + Template spreadsheet to export Plan of Actions and Milestones data from SRP.
* ManualScansTemplate.xlsx
  + Template spreadsheet for inputting Manual Scan data, when no xml STIG is available (e.g. Dot Net Framework 1 to 3.5).

## 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 – RMF x.x.x.accdb and the back end database is called Scan Results Processor – RMF x.x.x 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”. You must 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 (not available on NMCI). 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”. With the use of the Select BackEnd functionality, it is easy to use one front end that can easily connect to multiple back end databases. The POAM template should be in the same folder as the front end 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.



When first opened, the database will execute an update of the back end database if any changes have been made. This would only occur when using a newer version of the front end. 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.

Another check looks to see if this version of the database matches the release version on Github.com. Clicking Yes will open the default browser and go to github.com and the latest release page for Scan Results Processor – RMF. It will also close the database. Clicking No will continue to the MainGui.

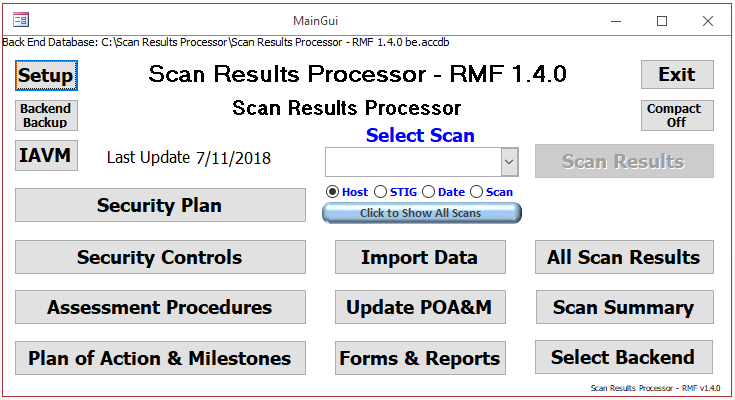


Another check looks to see if the CCIs have been updated within the last six months. STIGs are updated quarterly and can be found on the iase.disa.mil web site. Clicking Yes will open the default browser and go to github.com and the latest release page for Scan Results Processor – RMF. It will also close the database. Clicking No will continue to the MainGui. There is no need to replace the entire database. Download the CRPCCIUpdate.csv file and place it in the same directory as the backend database. Then from the Setup screen, click Update CCIs.



# MainGui

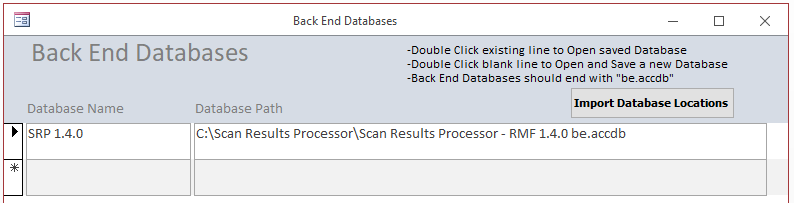
The MainGui will be the base of operations for the SRP.



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

## Back End Databases

Take note of the location of the back end database, which is shown at the top of the window. If you want to connect to a different back end database, click the Select Backend button.



The Back End Databases form allow the user to select or add back end databases. Double clicking in either the Database Name or Database Path field for an existing record will load the back end database chosen. Double clicking in either the Database Name or Database Path field for a new record will bring up the Windows File Open dialog box allowing the user to choose the location of the back end database. If new tables have been created in newer versions of the database, then it is possible to get an expected error similar to the following:



Enter a name for the back end database selected in the Back End Database Nickname form.



Successful links will generate the following message:

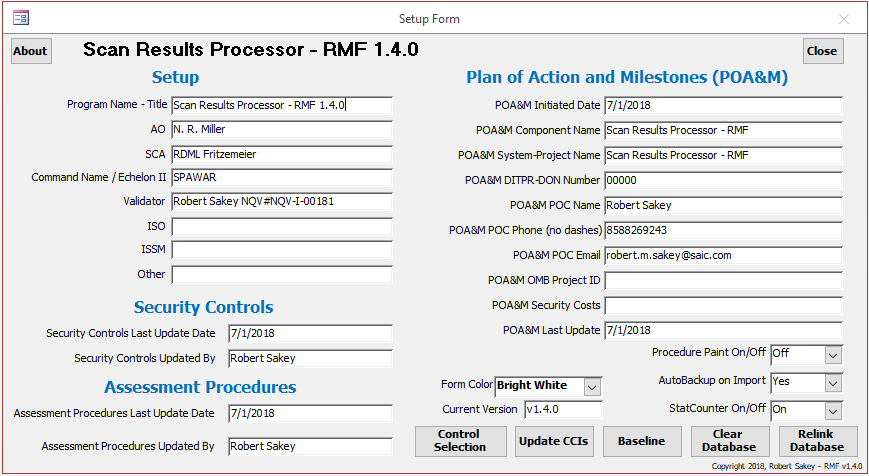


New versions of the front end database do not have the Back End Database records found in the Back End Databases form. To import the back end databases, click on the Import Database Locations button (twice). Select the location of a front end database from the Microsoft File Open dialog. After import, this message will display:



## Setup Form

From the MainGui form, click the **Setup** button to open the Defaults Form.



**Example of the Defaults Form**

### Setup data

Enter Setup information. The Program Name – Title will appear on the MainGui and many reports and windows within the SRP.

### Security Controls

Enter Last Update Date and Updated By information for the Security Controls.

### Assessment Procedures

Enter Last Update Date and Updated By information for the Assessment Procedures.

### POA&M

Enter POA&M information. This information is typically found in the header of the POA&M.

### Form Color

This drop down box allows the user to select the color of the MainGui.

### Procedure Paint On/Off

This drop down box turns the color on or off for the Assessment Procedures button on the Scan Results Form. This drop down box also exists on the Scan Results Form. It is recommended that this be kept at “Off” or “0” for normal operations.

### AutoBackup

This drop down box sets the status for Auto Backup when importing scans. When set to “Yes”, an automatic backup of the backend database will be created. When set to “No” an automatic backup of the backend database will not be created. The default value is “Yes”.

### Control Selection

This allows the selection of Controls, Assessment Procedures and Overlays.

#### 800-53 Control Selection

Select Confidentiality, Integrity and Availability levels. Closing the selection window will reset the applicable Security Controls after clicking Yes on the following message:



**Note: This will remove any applied Overlays.**

#### Setup Overlays

If you need to apply overlays, first make changes to the Security Controls, exit the Selection window, then return to the Control Selection and click on Setup Overlays.



Green highlight shows the applicability of the specific overlay. For example, the applicability of the Classified and Privacy Overlays above shows for AC-11 and AC-20(3). The Yes field for each control is highlighted along with the Classified row of data (top row) and the Privacy row of data (second row). Not all Overlays have Control Text, Supplemental Guidance or Parameter Values, which is why there are highlighted blank fields. Select an Overlay by clicking the specific Apply Overlay button. The text and color of the button changes depending on whether an overlay has been applied or not. You can click more than one. A message will pop up every time an Overlay is applied. Do not apply both Cybersafe A and Cybersafe B.



#### Open Controls Report

The Open Controls Report shows a list of Security Controls associated with the selected Confidentiality, Integrity and Availability

#### Open Controls Report - Details

The Open Controls Report – Details shows a list of Security Controls associated with the selected Confidentiality, Integrity and Availability along with Control Text and Supplemental Guidance.

#### Open Controls Report - Procedures

The Open Controls Report - Procedures shows a list of Assessment Procedures associated with the selected Confidentiality, Integrity and Availability along with CCIs, CCI Definitions, Implementation Guidance and Assessment Procedures.

#### Open IA Controls Report

The Open IA Controls Report shows a list of Security Controls associated with the selected Confidentiality, Integrity and Availability mapped to associated IA Controls.

#### Open Form

The 800-53 Controls Form shows the data associated with the Security Controls. It also allows the user to add additional controls by putting the letter “A” into any blank CIA field. Make sure to also put a “Y” into the Selected Control field.

#### Open Common Controls Report

The Open Common Controls Report shows a list of Security Controls associated with the selected Confidentiality, Integrity and Availability and which ones are Common Controls.

#### Remove Additional Controls

The Remove Additional Controls will remove the letter “A” from the 800-53 Controls Form. Removing the “Y” from the Selected Control field will require the user to close out and select the “Yes” from the Seet Security Controls dialog box.

### Update CCIs

This updates the relationship between vulnerabilities found in STIGs and CCIs. This is updated every quarter with the release of a new STIG zip compilation file. This requires the existence of a specially compiled csv file named “SRPCCIUpdate.csv”. To create the SRPCCIUpdate.csv, do the following:

1. Open the STIG Viewer.
2. Select all STIGs.
3. Right click 🡪 Remove highlighted STIG(s).
4. File 🡪 Import STIG.
5. In Open Dialog, change File Type to STIG ZIP File(\*.zip).
6. Select latest SRG-STIG\_Library zip file.
7. Click Open.
8. Click Ok to All to overwrite STIGs if dialog box appears.
9. Click the + in the STIGs section.
10. Select FileName and deselect Name.
11. Scroll to the bottom of the list.
12. Select all Benchmarks, if any exist.
13. Right click 🡪 Remove highlighted STIG(s).
14. Right click 🡪 Check All.
15. Click Export 🡪 Spreadsheet(.csv). \*\*\*It should be noted that the Export function of the STIG Viewer is not robust. You may have to use STIG Viewer 1.2 in order to get your own file. For now on, a SRPCCIUpdate.csv file will be included with each SRP release.
16. Select Name (good practice to name it SRPCCIUpdate{Date}.csv and Location (front end database location) to save file.
17. Open file.
18. Remove all columns except for Vuln ID, Severity, Group Title, Rule ID, STIG ID, Rule Title, STIG and CCI.
19. Remove all rows above header row.
20. Remove rows at bottom without data (~~~~~UNC~~~~~”)
21. Do Search and Replace for the following in the STIG column only:
    1. Security Technical Implementation Guide to STIG
    2. Secure Technical Implementation Guide to STIG
    3. Security Implementation Guide to STIG
    4. STIG (STIG) to STIG
    5. Security Requirements Guide to SRG
    6. SRG (SRG) to SRG
22. Sort by CCI column A-Z
23. Save and close file.
24. Copy file and rename to SRPCCIUpdate.csv.
25. Backup current database
26. Click Update CCIs button on Setup form in database.
27. When complete, it is a good idea to set Compact On prior to closing database.

### Clear Database

This clears all data from the backend database. Be judicial about doing this as it will remove your data.

### Baseline

This marks findings as baselined. Differences between baselined and non-baselined findings can be found in a report. This will allow the user to create a POAM import file that only has new findings in it from the last time a baseline was created in eMASS.

### Relink Database

If the Scan Results Processor was moved or renamed, then the first thing that should be done is to relink the database. This is rarely needed as the Select Backend functionality from the MainGuid should take care of all issues. 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.



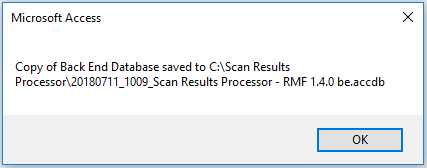
After all linked table are successfully refreshed, click the close button.

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.

## Backend Backup

The Backend Backup button allows a quick way of making a copy of the backend database.



## Exit

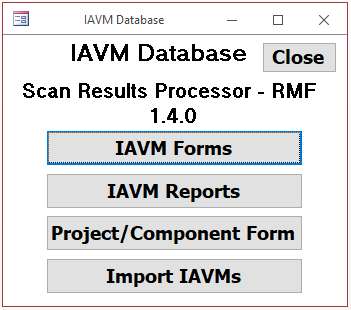
It is preferable to use the Exit button to exit the database.

## Compact Off/On

The Compact Off/On button allows the user to select whether the database will be compacted after clicking the Exit button. It is recommended that the database be compacted at least weekly. This does not compact the back end database. To compact the back end database. Close the front end database. Open the back end database to be compacted. Select Database Tools from the menu then select Compact and Repair Database from the Microsoft Office ribbon. Then click the Exit Database button to exit. The back end database will grow considerably with each import. A compact will reduce the size of the database.

## IAVM

The IAVM button allows the user to access optional Information Assurance Vulnerability Management functionality.



The IAVM Main form allows the user to access IAVM Forms, IAVM Reports, the Project Form, and the ability to import IAVAs and IAVBs.

### Project Form

The Project Form is a list of Projects or Components of the system.



### IAVM Forms

Clicking on the IAVM Forms button opens the IAVM Form Selection Form.



Select an IAVM Status of either Active or All. All is the default value if nothing is selected. Then select either the Open IAVM Form button or the Open IAVM Project Form.





The IAVM Project Form shows all IAVs associated with Projects/Components. One row for each IAV/Project/Component. Entering check marks in the Applicable, Lab Applied, and Deployed check boxes will mark the IAVs different colors: Gray for Not Applicable (default), Red for Applicable but not Applied, Yellow for Applicable and Applied in the Lab, but not Deployed, and Green for Deployed.

### IAVM Reports

Clicking on the IAVM Reports button opens the IAVM Report Selection Form.



Select an IAVM Status of either Active or All. Select an Applicable of Applicable or All. All is the default value if nothing is selected. Then select either the Open IAVM Report button or the Open IAVM Project Report. When selecting Applicable in the Applicable drop down box, the IAVM Project Report will filter for only those IAVMs that are checked as Applicable.





The IAVM Project Report shows all IAVs associated with Projects/Components. One row for each IAV/Project/Component. Entering check marks in the Applicable, Lab Applied, and Deployed check boxes on the IAVM Project Form will mark the IAVs different colors on this report: Gray for Not Applicable, Red for Applicable but not Applied, Yellow for Applicable and Applied in the Lab, but not Deployed, and Green for Deployed.

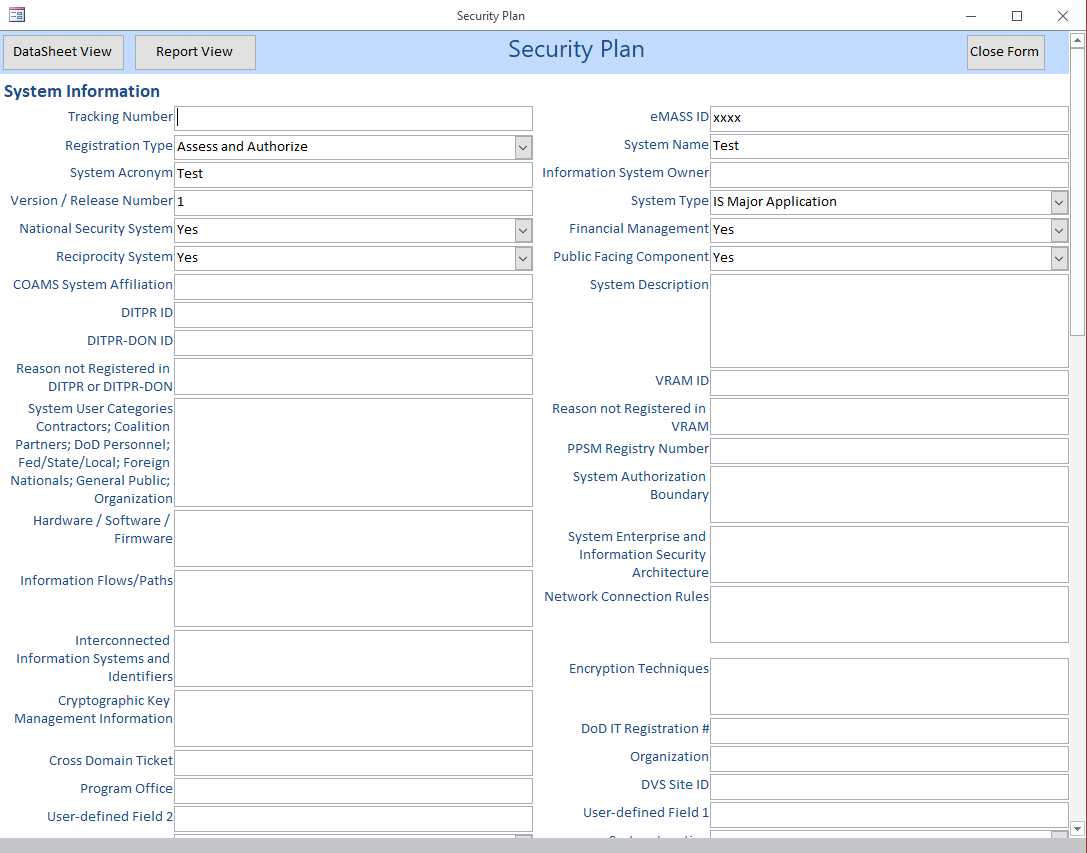
### Import IAVMs

The Import IAVMs button will run code that will import the latest iavms.xls from the IAVM web site. Make sure that the iavm.xls file is located in the same directory of the front end database. The file can be downloaded from <https://iavm.csd.disa.mil/>. Click the Notices button, then click Search Notices. From the Search IAVM Notices screen, check the Include non-active notices check box, then click the Download Excel Summary button. This will download a full list of all IAVs as iavm.xls.

Also, click this button if any changes are made to the Project/Component form.

## Security Plan

The Security Plan matches the fields for the Security Plan in eMASS. You should only create one record for this form.



The DataSheet View button allows the user to enter and review data in a spreadsheet format. The Report View allows the user to create a report of the Security Plan.

## Security Controls

The Security Controls Form allows the user to provide status for selected security controls. Many of the fields on this form are required for other reports. Entering any data in the Inherited From field automatically marks that Security Control and its associated Assessment Procedures as Inherited. Deleting any value in the Inherited From field automatically removes the inheritance from that Security Control and its associated Assessment Procedures. Selecting “Yes” in the Not Applicable field will also mark all associated Assessment Procedures as Not Applicable. Selecting “No” in the Not Applicable field will mark all associated Assessment Procedures as not Not Applicable.

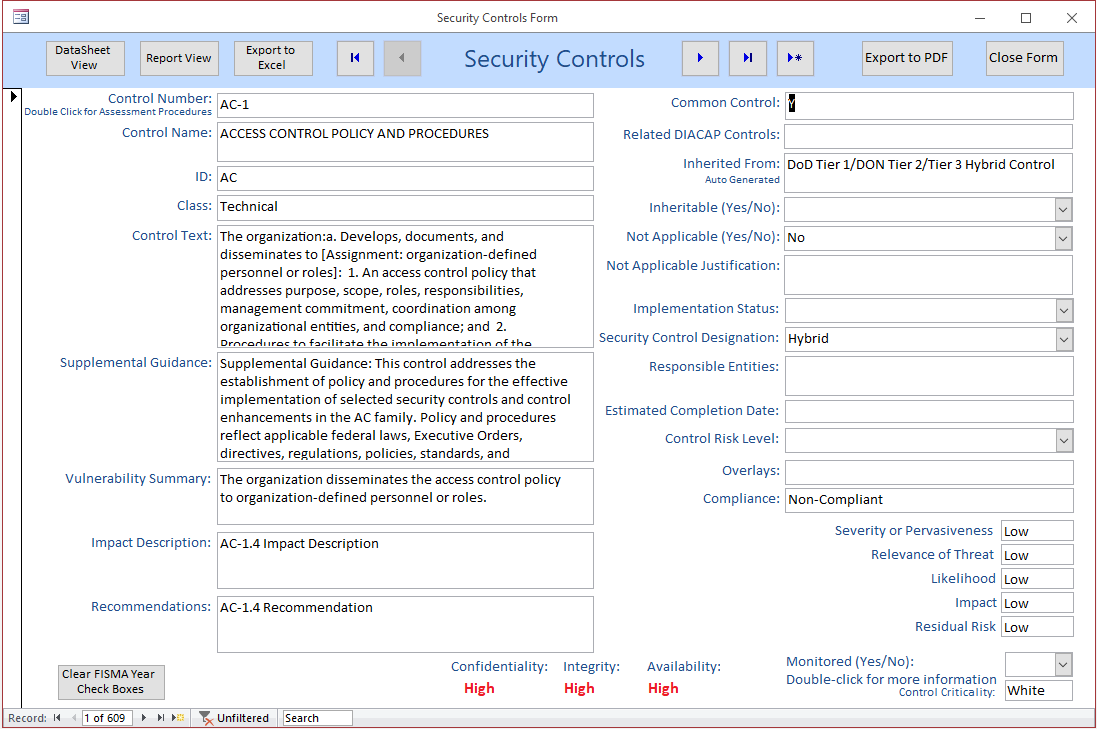
Changes to the Inherited From, Inheritable, Not Applicable and Not Applicable Justification fields overwrite the same fields on the Assessment Procedures Form. If the Inherited From field on the Assessment Procedures Form has “Tier 1” or “Tier 2” in it, it will not be updated, as these need to be updated manually.

The values for Confidentiality, Integrity and Availability in addition to the Overlays field show how each Security Control is relevant. The CIA values are the lowest values for each control. For a High, High, High categorization, a Low or Moderate value means that the particular Security Control is also relevant to Low or Moderate categorizations.

The DataSheet View button allows the user to enter and review data in a spreadsheet format. The Report View allows the user to create a report of the Security Controls. The Export to Excel button will export the Security Controls query to Excel. To change the format of the export for the future, edit the Security Controls.xlsx file in the same folder as the front end database. The Export to PDF button will create a pdf of the Report presented in the Report View.

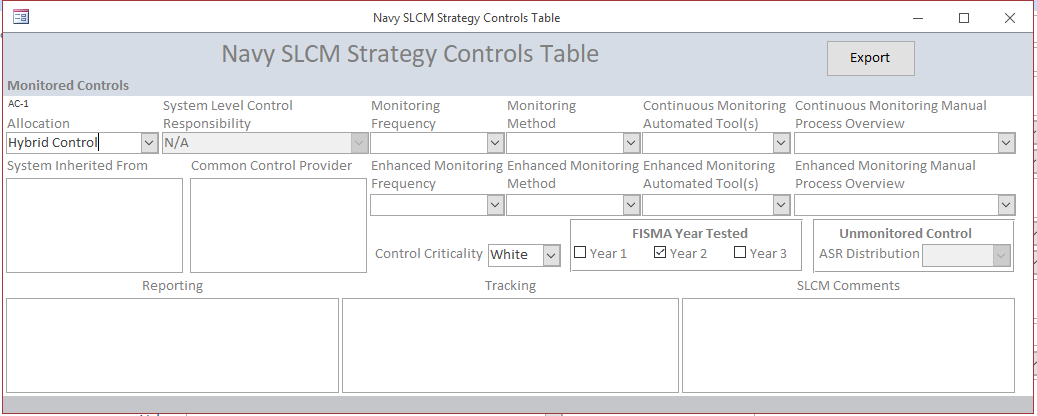
The Clear FISMA Year Check Boxes button will clear the FISMA Year 1, 2 and 3 checkboxes found on the SLCM form detailed below.

The values for Severity, Relevance, Likelihood, Impact and Residual Risk are taken from the highest value from ongoing findings associated with each Security Control. The contents of the Vulnerability summary, Impact Description and Recommendations fields are concatenations of all the values from ongoing findings associated with each Security Control.



### Monitored Control Information

The Monitored Control Information form is used to complete the Monitored Control Information sheet associated with the Navy System Level Continuous Monitoring Controls Table. Many of the fields on this form are dependent upon the value in the Allocation and Monitoring Method fields. Values for the Control Criticality field are automatically generated based on the colors of the Control Criticality diamonds associated with the Security Controls in eMASS. These controls are monitored annually or more often. While the Monitored field is marked “Yes” on the Security Controls form, the ASR Distribution field is grayed out. Use the FISMA Year Tested fields for FISMA reporting. Clicking the Export button will produce a spreadsheet to match the Navy\_SLCM\_Strategy\_Controls\_Table template with two tabs, Monitored Controls and Unmonitored Controls.



### Unmonitored Control Information

The Monitored Control Information form is used to complete the Unmonitored Control Information sheet associated with the Navy System Level Continuous Monitoring Controls Table. Unmonitored Controls can be monitored as part of the annual review in Year 1, Year 2 or Year 3. While the Monitored field is marked “No” on the Security Controls form, the ASR Distribution field is enabled and highlighted yellow and all other fields are grayed out. Use the FISMA Year Tested fields for FISMA reporting.

## Assessment Procedures

The Assessment Procedures Form allows the user to provide status for assessment procedures associated with selected security controls. Many of the fields on this form are required for other reports. Entering any data in the Inherited From field does not automatically mark that Security Control as Inherited. Deleting any value in the Inherited From field does not automatically remove the inheritance from that Security Control. Selecting “Yes” in the Not Applicable field will not mark the associated Security Control as Not Applicable. Selecting “No” in the Not Applicable field will not mark the associated Security Control as not Not Applicable.

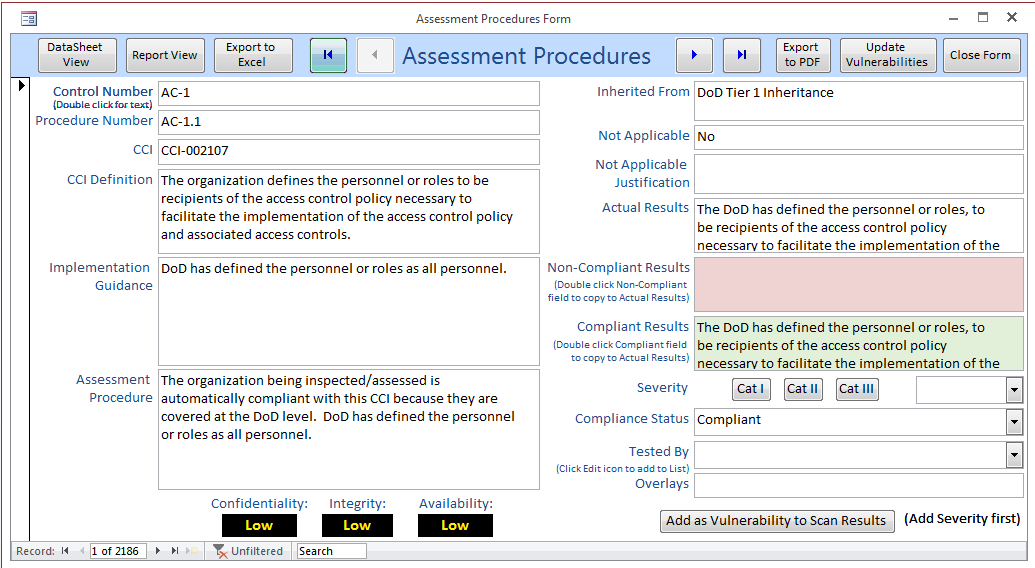
After scans are imported, a concatenation of all the open findings associated with a particular Assessment Procedure can be created in the Non-Compliant Results field by clicking the Update Vulnerabilities button. The same will be done for closed findings in the Compliant Results field.

Selecting the Cat I, Cat II or Cat III buttons or selecting from the drop down box will enter a severity for the finding.

The values for Confidentiality, Integrity and Availability in addition to the Overlays field show how each Assessment Procedure is relevant. The CIA values are the lowest values for each procedure. For a High, High, High categorization, a Low or Moderate value means that the particular Assessment Procedure is also relevant to Low or Moderate categorizations.

Clicking the **Add as Vulnerability to Scan Results** button will add the procedure as a vulnerability to the scan results with a ScanID of 1 and Host name of 800-53 Rev4. The Severity needs to be added first. This allows any of the Assessment Procedures to be added as a Vulnerability and treated like any other vulnerability on a STIG.

The DataSheet View button allows the user to enter and review data in a spreadsheet format. The Report View allows the user to create a report of the Assessment Procedures. The Export to Excel button will export the Assessment Procedures query to Excel. To change the format of the export for the future, edit the Assessment Procedures.xlsx file in the same folder as the front end database. The Export to PDF button will create a pdf of the Report presented in the Report View.



## Plan of Action & Milestones

The POA&M can be opened by clicking the **Plan of Action & Milestones** button on the MainGui. This report is comparable to the old System POA&M. 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. Header information can be entered in the Setup screen.



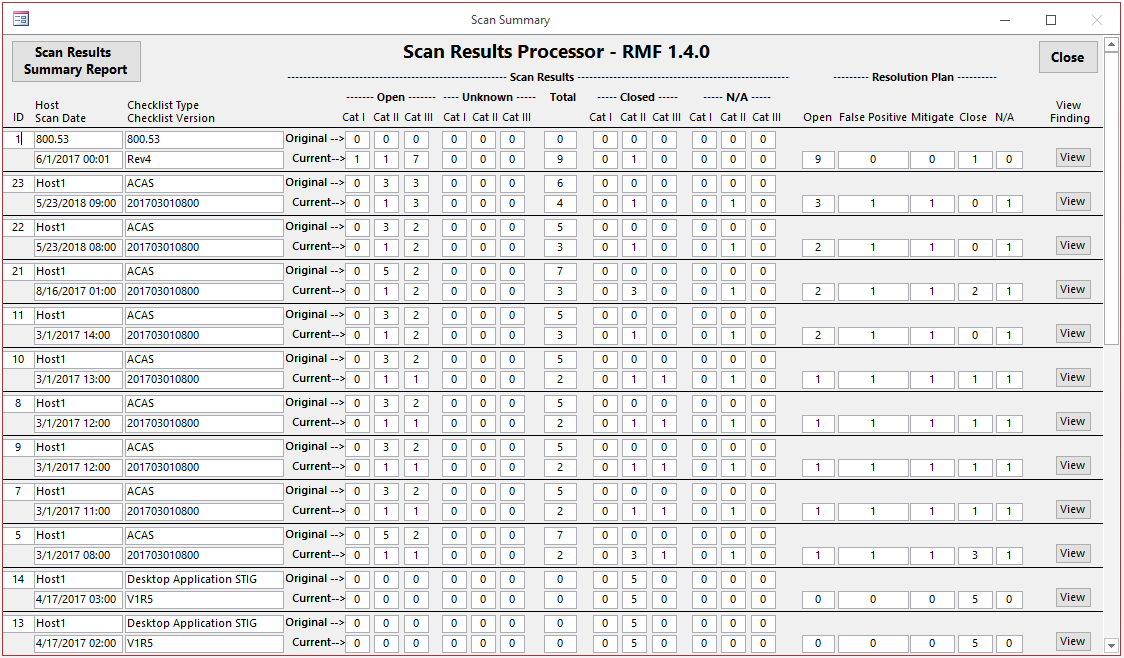
## Update POA&M

The Milestone fields on the POA&M can be updated by clicking the **Update POA&M** button on the MainGui.

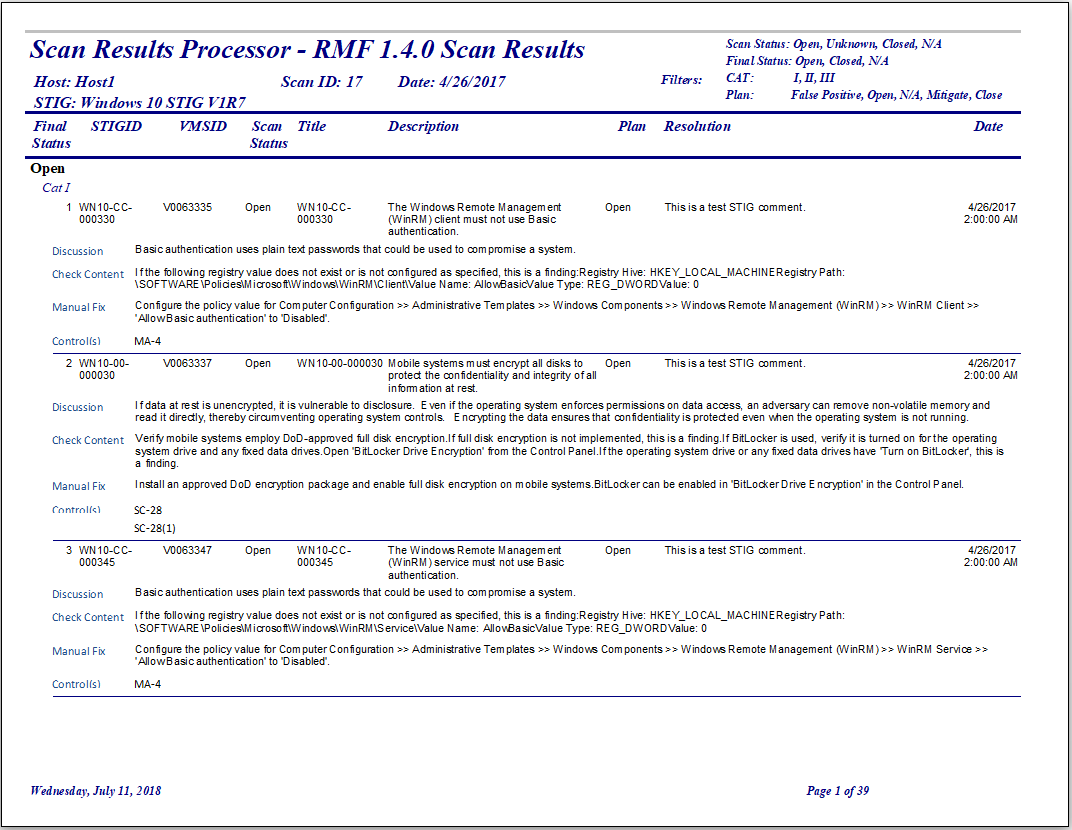


## Scan Summary

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.

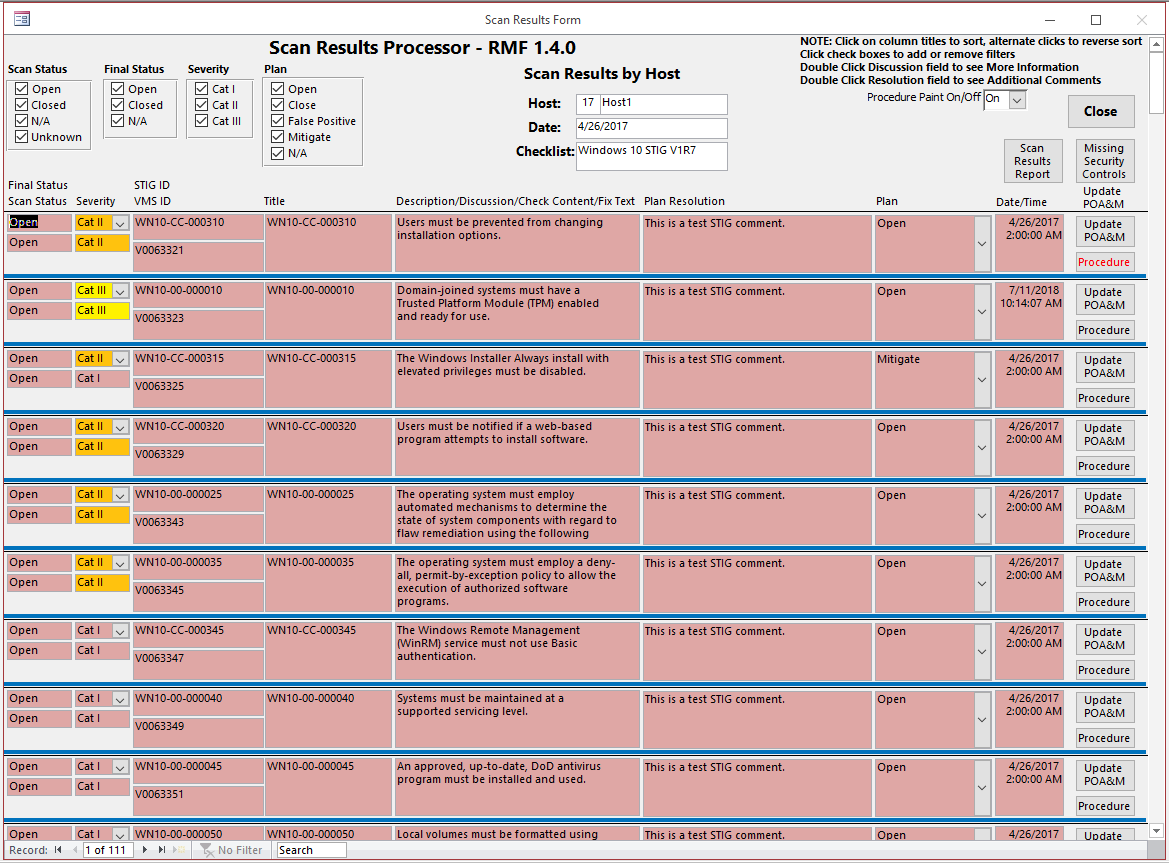


There are two reports available on the Scan Summary Form, a Scan Results Summary Report, which shows the contents of the Scan Summary Form and a Scan Results Report, which shows a report similar to the one on the Scan Results Form. This can be accessed by clicking the View button next to each scan.



## Scan Results

The Scan Results button will become enabled after a Host is selected from the Select Host drop down box. To access a particular host’s scan results, select a host from the MainGui’s “**Select Host**” drop down box and click the **Scan Results** button. The Select Host drop down box can be filtered in various ways. To see only the latest scan for a particular host and checklist, click the “**Click to Show only Latest Scans**” button. It will change to “**Click to** **Show All Scans**”. The Host can also be sorted by selecting one of the radio buttons, Host, STIG, Date or Scan (ID).



### Viewing Vulnerabilities

From the Scan Results Form, 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 filtered 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.

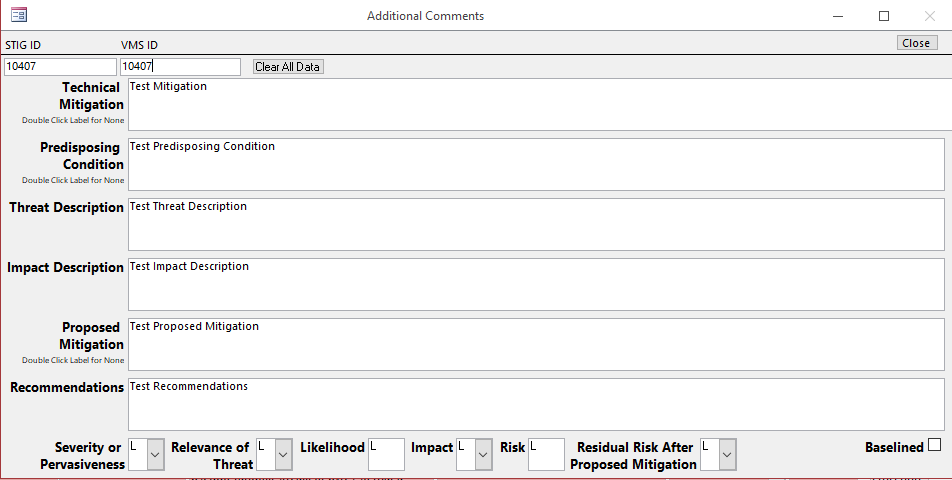
### Updating Vulnerabilities

The object of this form is to provide a status for the compliance of each vulnerability through the development life-cycle. Each vulnerability can be updated with amplifying information. The **Severity** and **Plan** can be changed via drop down combo boxes. The **Severity** cannot be changed unless the corresponding **Plan** has been changed to **Mitigate**.

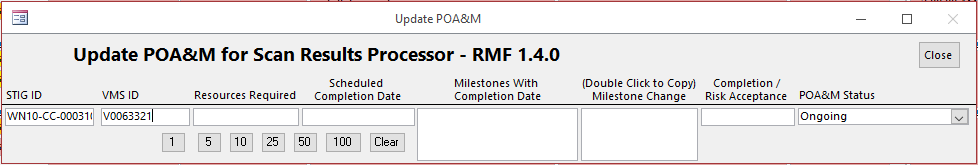
In order to see the Discussion, Check Content, Fix Text and STIG Comments fields, double click the Description. The STIG comments are specific to each scan, but the Discussion, Check Content and Fix Text fields are the same for all scans for each vulnerability. The **Plan Resolution** field will be filled in with the **STIG Comment** during a STIG import if the existing **Plan Resolution** is blank. Otherwise, it will not be overwritten.



The “Plan Resolution” offers a wholly editable textbox to enter specifics as to the 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 ancillary form that will allow you to enter fields of data associated with the eMASS Risk Assessment Report (RAR). By double clicking the label for Technical Mitigation, stock answers will appear. All data from the form can be cleared by clicking the Clear All Data button. The Baselined check box will show whether a particular vulnerability has been baselined. Baselining should be done from the Setup screen.



In addition, the POA&M can be updated with Milestone information by clicking the **Update POA&M** button on this form or the MainGui. Although not recommended, the **POA&M Status** of a vulnerability can be changed from this form. Only do this if updating the Plan or a subsequent import does not mark the Status correctly. It should be noted that when importing vulnerabilities into eMASS, if the vulnerability already exists and the **Milestone Change** field is not blank, then the **Milestone** in eMASS will be updated.



The **Scan Status** field shows the status of the vulnerability during import. It will never change. Making changes to the **Plan** field will change the **Final Status** field for this scan. The **Plan** field can be changed to **False Positive**, **Mitigate**, **N/A**, **Close** or **Open**. The Final Status will change to **Open**, **Closed** or **N/A**. Changes to the Plan will also make changes to the POA&M Status. The **POA&M Status** can be **Ongoing**, **Completed**, **N/A**, **False Positive**, **Inherited – Ongoing** or **Inherited – Completed**. The **POA&M Status** is automatically marked as Inherited only if ALL the CCIs associated with the vulnerability are marked as Inherited.

Due to RMF requirements, vulnerabilities must be associated with NIST 800-53 Security Controls. Clicking the **Procedure** button brings up a small dialog box from which one or more CCIs/Assessment Procedures can be associated with a particular vulnerability.

**Warning**: If an Open Vulnerability has no Security Control associated with it, the RAR will not show it and the POA&M will show it but with an empty field for Security Control.



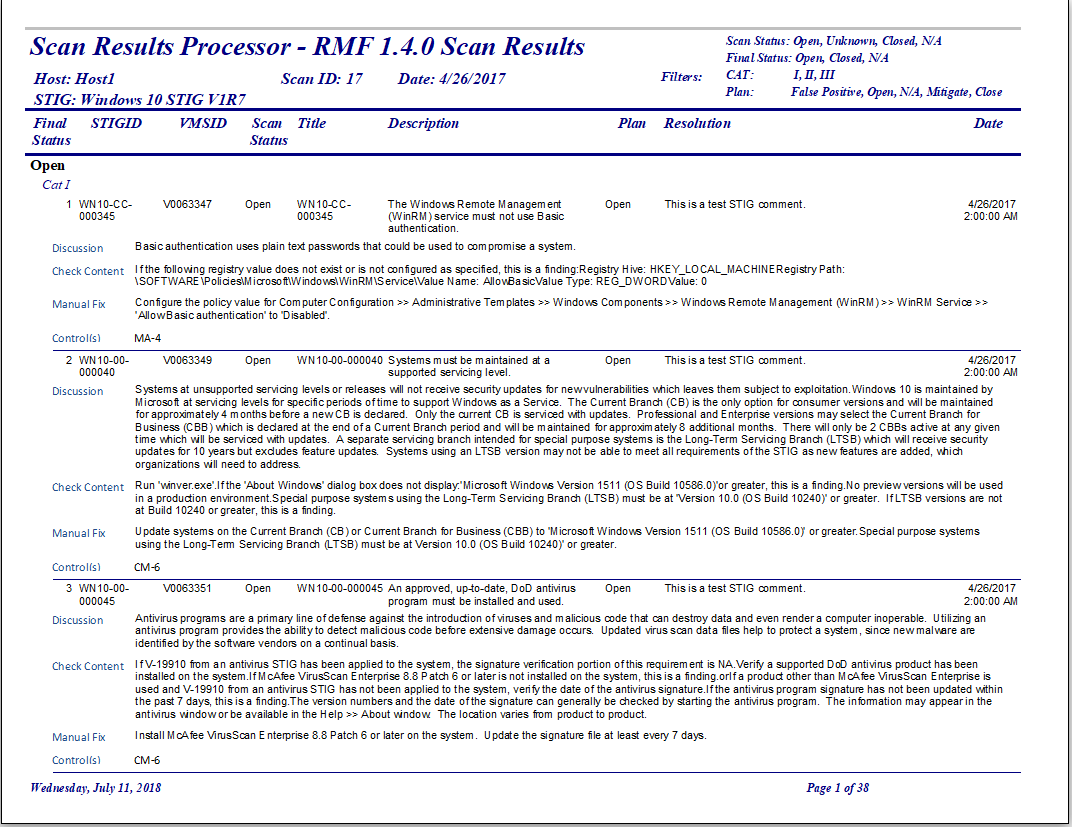
**Example of the IA Controls Association Dialog Box**

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

Changes to the Plan and subsequent imports of matching STIGs for different hosts should (perfection is a goal we can only strive for) mark the **POA&M Status** appropriately. For example, if Windows 10 STIG results are imported for two different Hosts, then if there are any open vulnerabilities on one Host, then the **POA&M Status** should be marked as **Ongoing**. If a vulnerability is **Open** on more than one Host, and a subsequent import closed the vulnerability on one Host, the **POA&M Status** should still be Ongoing. The **POA&M Status** shouldn’t change to **Completed** until the vulnerability is **Closed** for All Hosts.

### Scan Results Report

A report showing the vulnerabilities on the Scan Results Form can be viewed by clicking the **Scan Results Report** button. The vulnerabilities can be filtered by selecting or unselecting the various check boxes on the Scan Results Form. The particulars filtered selected will appear on the upper right hand side of the report.



### Missing Controls

Clicking the **Missing Controls** button will show any vulnerabilities that have no CCI associated with it. Double clicking any vulnerability will move to that record on the form. It may show an associated vulnerability that is not on this particular scan. If that is the case, it is suggested that you utilize this form on the **All Scan Results Form**. There are two reasons that a vulnerability may have no CCI associated with it. First, there may actually be no CCI associated with the vulnerability. Not all STIGs have been updated to include CCIs. Second, there may be a CCI associated with the vulnerability, but it is not selected based on Confidentiality, Integrity or Availability. In addition, when the **Procedure Paint On/Off** is **On**, then the text of the **Procedure** button will show as Red.



### Procedure Paint On/Off

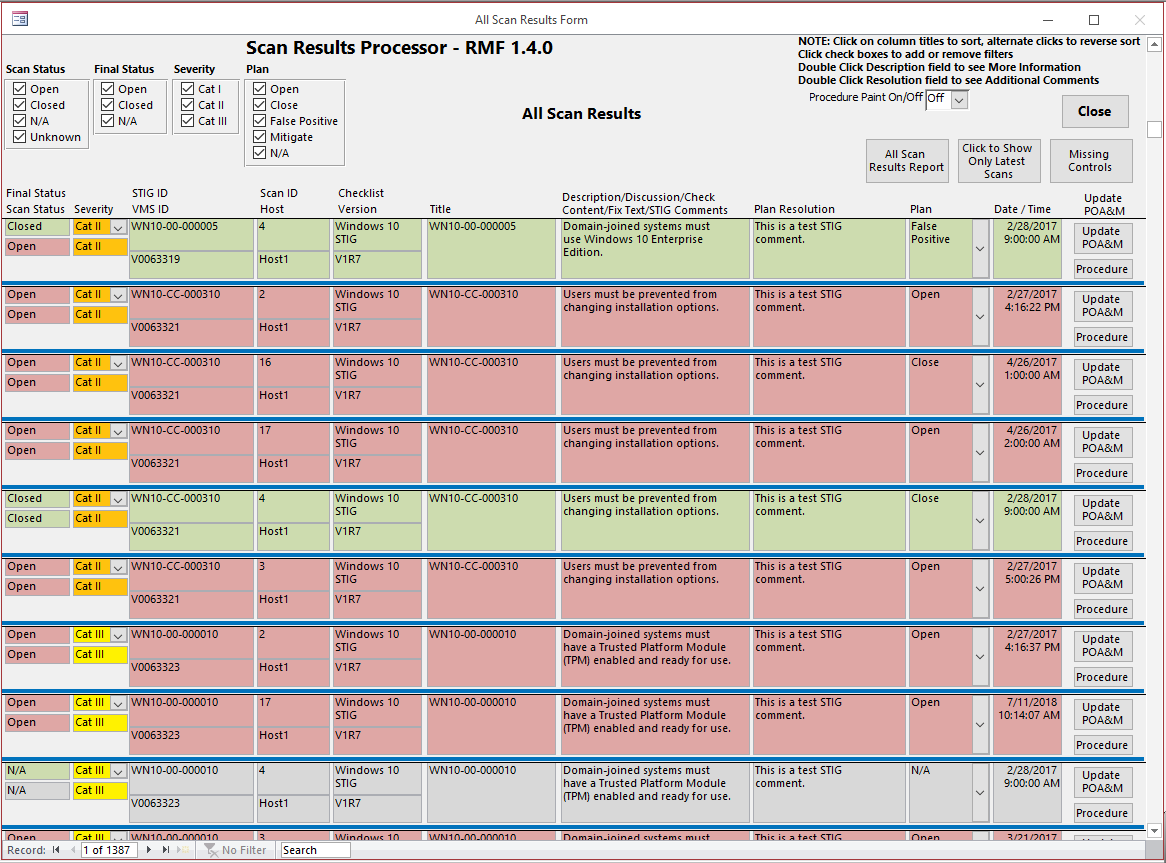
When the **Procedure Paint On/Off** is **On**, then the text of the Procedure button may change color. **Red** for missing CCI, **Blue** for Not Applicable CCI and **Green** for Inherited CCI. While this field is set to On, it repaints the screen constantly, making it annoying.

### Closing the Scan Results Form

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

## All Scan Results

The **All Scan Results Form** is similar to the **Scan Results Form** but the results for ALL scans are shown. Certain limitations have been set. The **Plan** field cannot be changed unless the scan is the latest for a particular host and scan type.



### All Scan Results Report

The **All Scan Results Report** will show All Open Findings.

### Click to Show Only Latest Scans

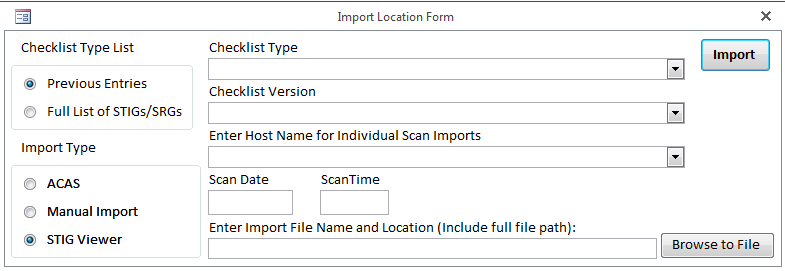
Clicking the **Click to Show Only Latest Scans** button will filter the form to show only the latest for each host and scan.

### Missing Controls

The **Missing Controls** button works the same as on the **Scan Results Form**.

## Import Data

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



Radio buttons allow the user to select two types of lists for the Checklist Type: Previous Entries and Full List of STIGs/SRGs. Radio buttons allow the user to select between three types of import formats: **ACAS**, **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

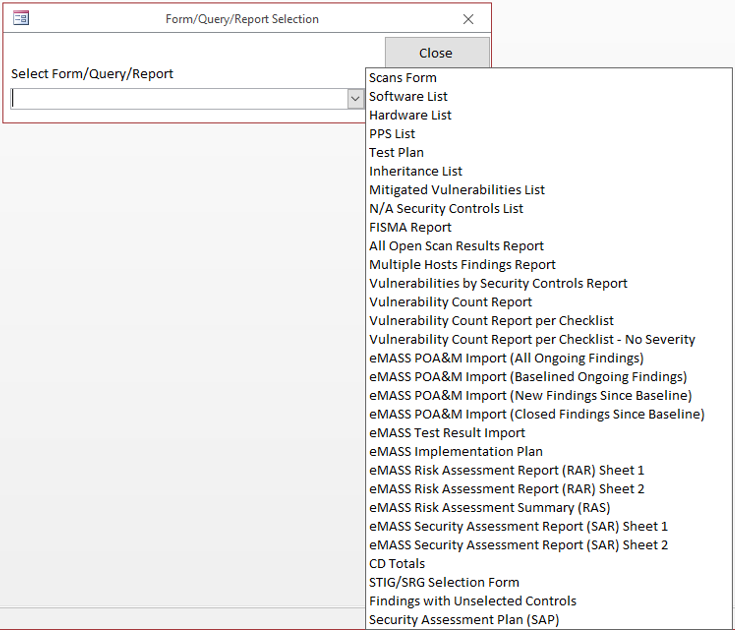
Select the scan data file by clicking the **Browse to File** button and choose the appropriate file (e.g. ManualScans.xlsx). Then click **Open** to continue back to the Import Location Form. From there click the **Done** button. On the Import Location Form, click the Import button.

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

When the scan data is successfully imported into the SRP database, the Scan Results Form will open, showing the imported scan.

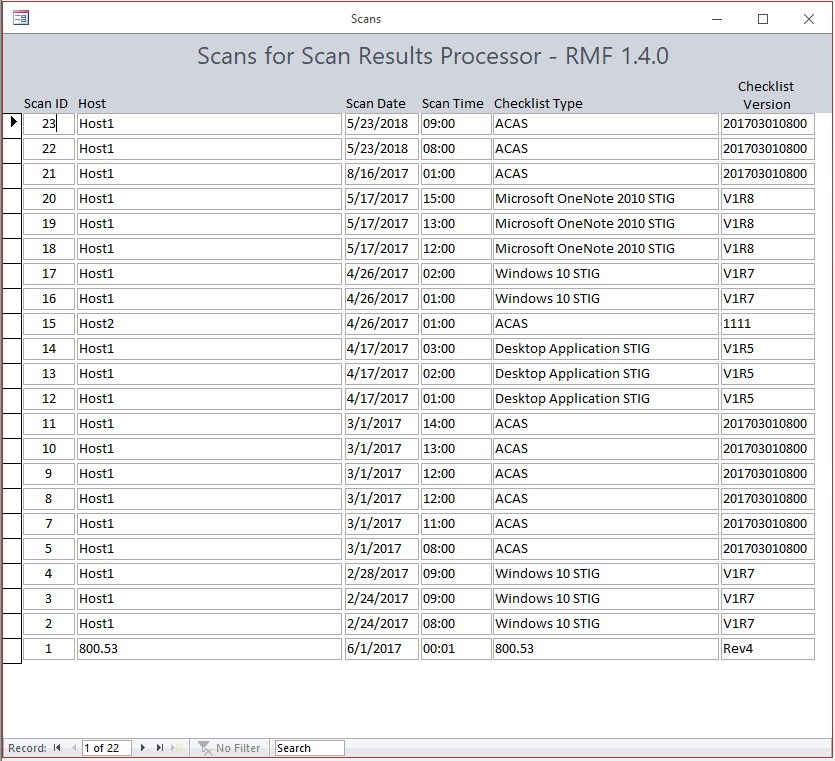
## Forms & Reports

The Forms & Reports button shows a list of Forms, Reports and Queries that provide more information about a scan or package.



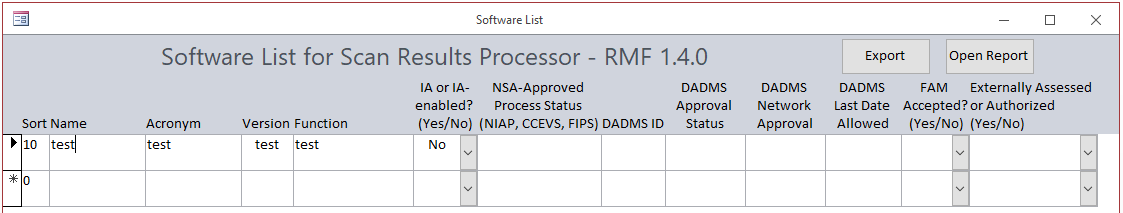
### Scans Form

The Scans Form shows all scans along with Date, Time, Host, Scan ID, Checklist Type and Checklist Version.



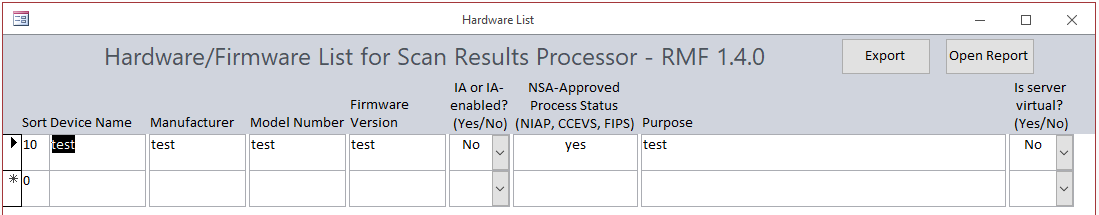
### Software List

The Software List shows software associated with a system. It can be exported out in a report that can be imported into eMASS.



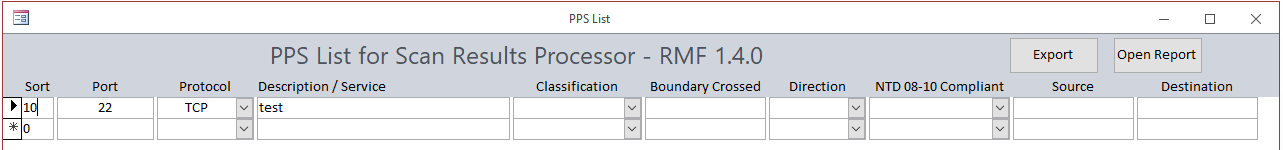
### Hardware List

The Hardware List shows hardware associated with a system. It can be exported out in a report that can be imported into eMASS.



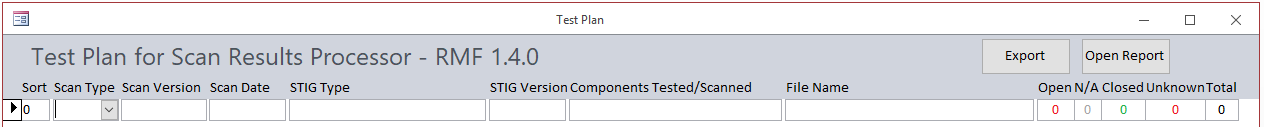
### PPS List

The PPS List shows ports, protocols and services associated with a system. It can be exported out in a report that can be imported into eMASS.



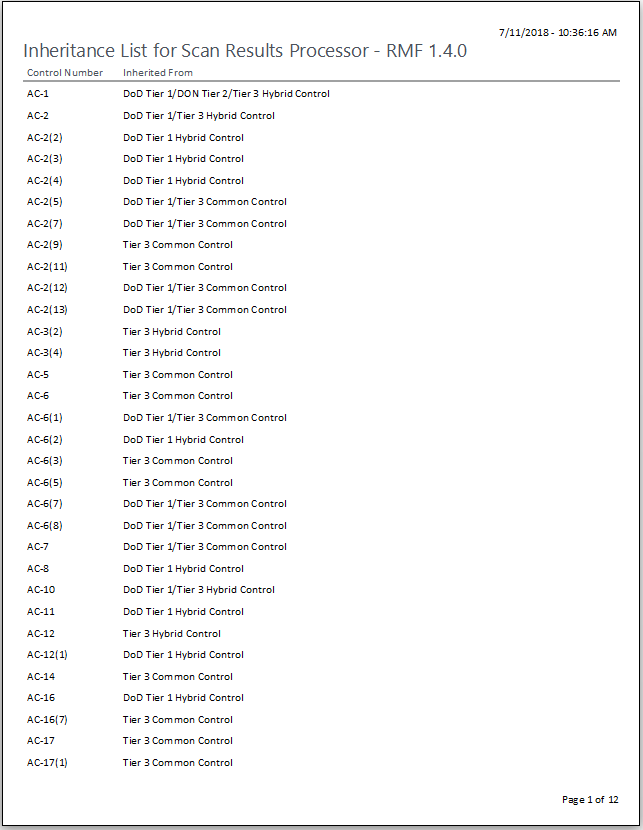
### Test Plan

The Test Plan shows the scans done for a system. It can also show the findings for each scan.



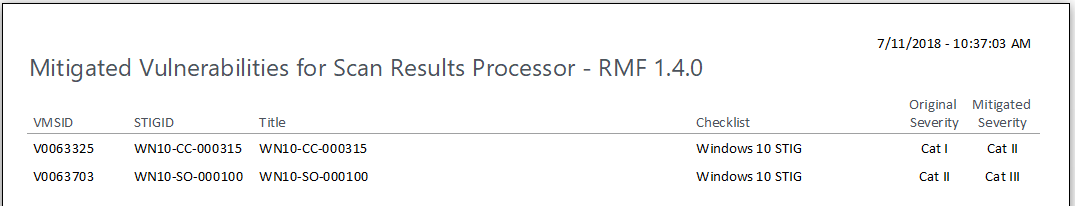
### Inheritance List

The Inheritance List shows all Security Controls listed as Inherited.



### Mitigated Vulnerabilities List

The Mitigated Vulnerabilities List shows all vulnerabilities that have had their **Severity** changed.



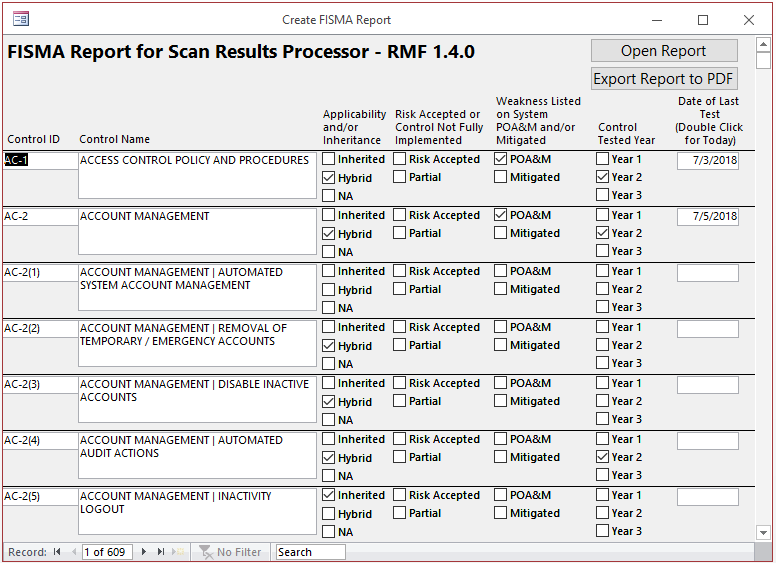
### N/A Security Controls List

The N/A Security Controls List shows all Security Controls that are marked as Not Applicable along with the Not Applicable Justification.



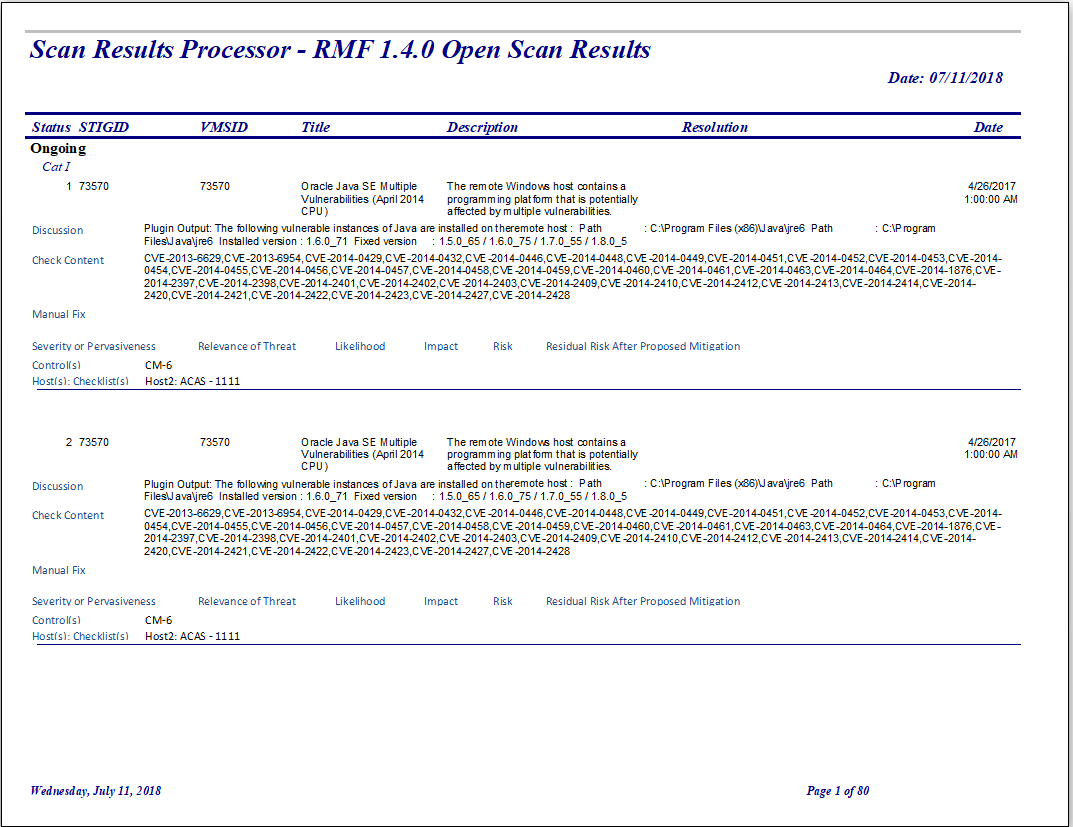
### FISMA Report

The FISMA Report shows an annual FISMA Report with some fields already filled in.



### All Open Scans Results Report

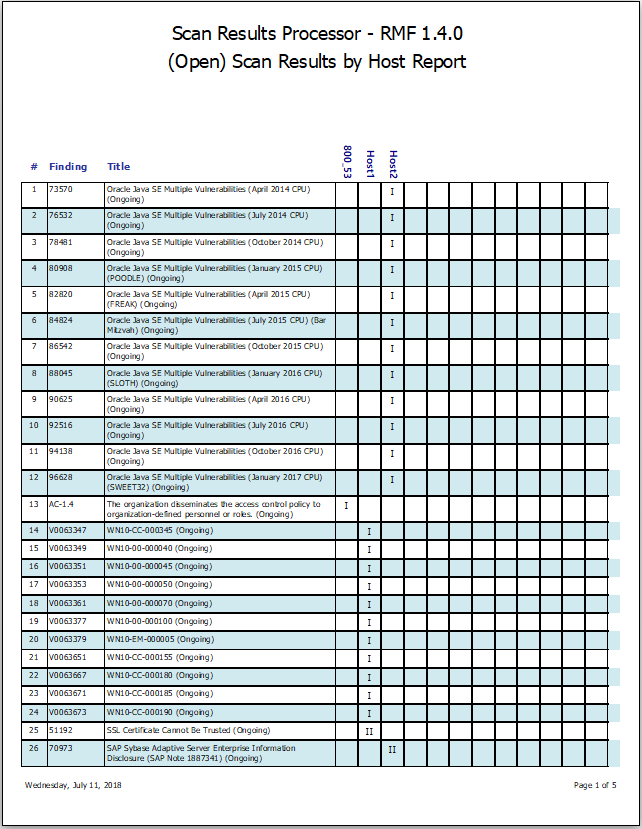
The All Open Scans Results Report shows ALL Open vulnerabilities.



### Multiple Hosts Findings Report

The Multiple Hosts Findings Reports shows findings across multiple hosts. Select Open, Closed or N/A findings.





### Vulnerabilities by Security Controls Report

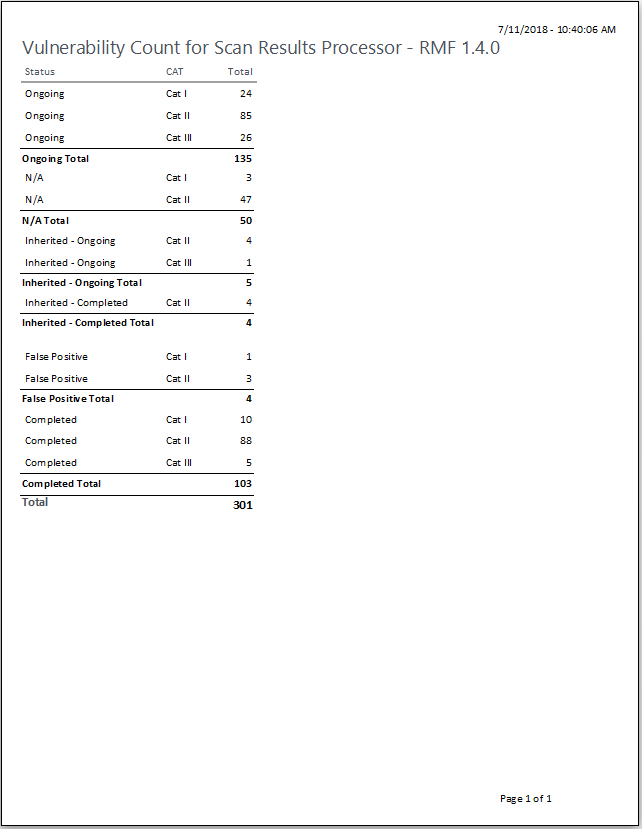
The Vulnerabilities by Security Controls Report shows a listing of all vulnerabilities and the associated Security Controls, Assessment Procedures and CCIs. First select Open, Closed and/or N/A.





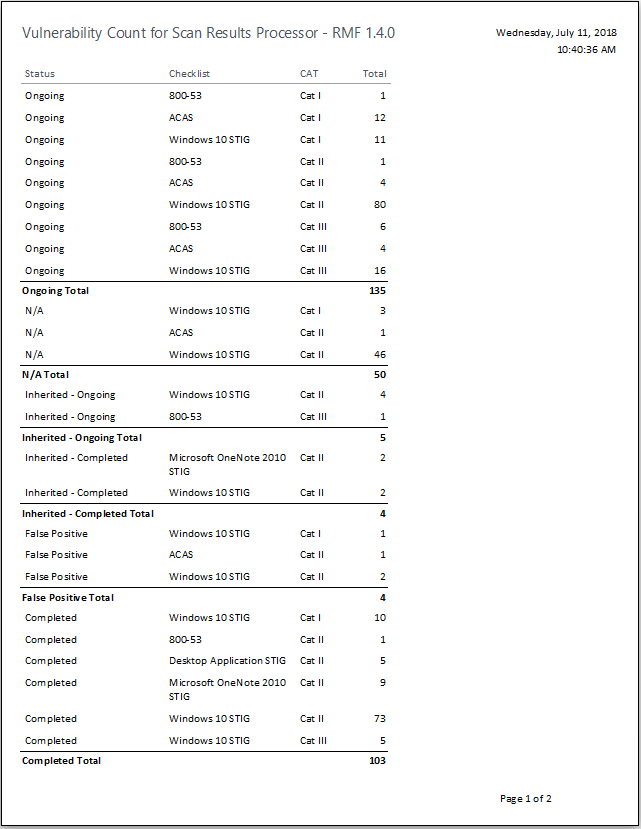
### Vulnerability Count Report

The Vulnerability Count Report shows the count of all vulnerabilities by status.



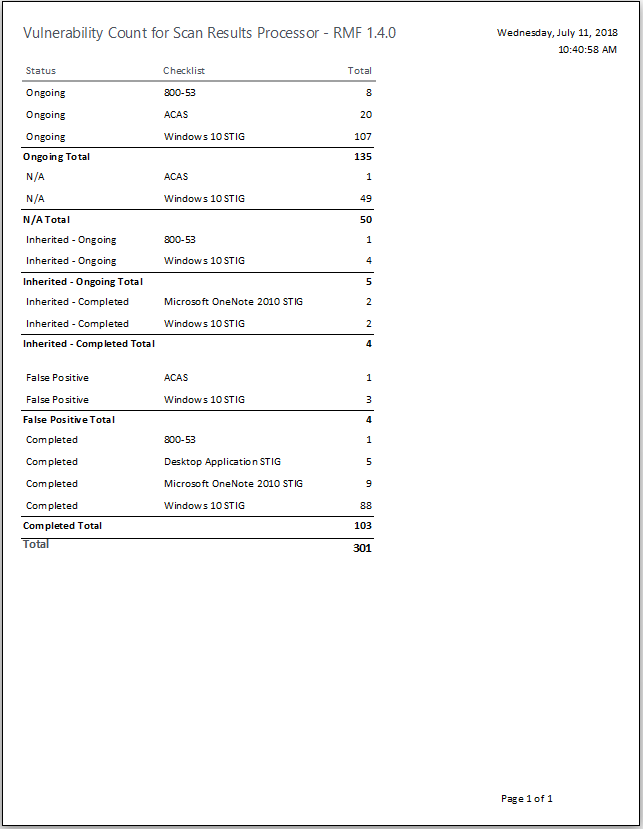
### Vulnerability Count Report per Checklist

The Vulnerability Count Report per Checklist shows the count of all vulnerabilities by status, severity and checklist type.



### Vulnerability Count Report per Checklist – No Severity

The Vulnerability Count Report per Checklist – No Severity shows the count of all vulnerabilities by status and checklist.



### eMASS Risk Assessment Report (RAR)

The RAR is exportable in the format expected for the RAR template.

### eMASS POA&M Import (All Ongoing Findings)

The eMASS POA&M Import (All Ongoing Findings) is in the format expected for the eMASS POA&M Import Template. This report shows all open findings.

### eMASS POA&M Import (Baselined Ongoing Findings)

The eMASS POA&M Import (Baselined Ongoing Findings) is in the format expected for the eMASS POA&M Import Template. This report shows only open findings that have been baselined.

### eMASS POA&M Import (New Findings Since Baseline)

The eMASS POA&M Import (New Findings Since Baseline) is in the format expected for the eMASS POA&M Import Template. This report shows only open findings that have not been baselined.

### eMASS POA&M Import (Closed Findings Since Baseline)

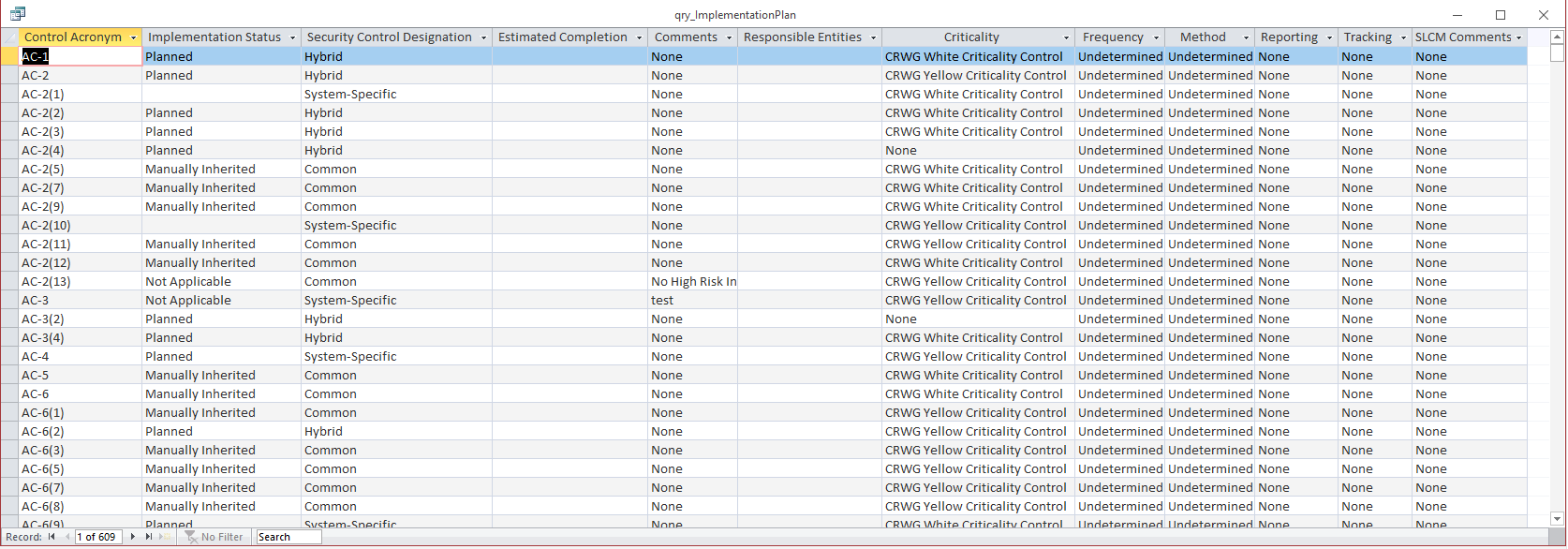
The eMASS POA&M Import (Closed Findings Since Baseline) is in the format expected for the eMASS POA&M Import Template. This report shows only closed findings that were marked as baselined. These findings would be marked as Closed in eMASS.

### eMASS Test Result Import

The eMASS Test Result Import is in the format expected for the eMASS Test Result Import Template. This report shows the compliance status of all CCIs.

### eMASS Implementation Plan (Assigned Security Controls)

The eMASS Implementation Plan (Assigned Security Controls) shows the implementation status of all assigned Security Controls along with SLCM information.



### eMASS Risk Assessment Summary

The eMASS Risk Assessment Summary shows Risk Assessment Summary of all assigned Security Controls.



### eMASS Security Assessment Report (SAR) Sheet 1

The eMASS Security Assessment Report (SAR) Sheet 1 shows the information for the first sheet of the SAR for import into the DoD SAR template.

### eMASS Security Assessment Report (SAR) Sheet 2

The eMASS Security Assessment Report (SAR) Sheet 2 shows the information for the first sheet of the SAR for import into the DoD SAR template.

### CD Totals

The CD Totals shows the count of findings as listed in the Certification Determination completed by the SCA representative.



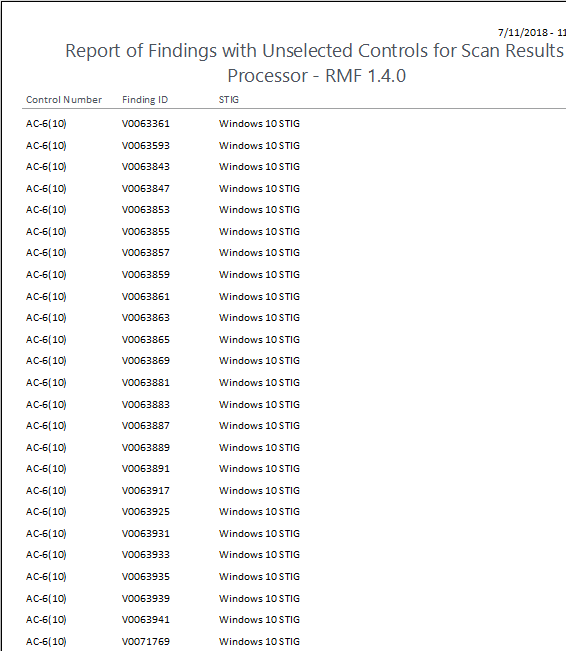
### STIG/SRG Selection Form

Select relevant STIGs on this form.



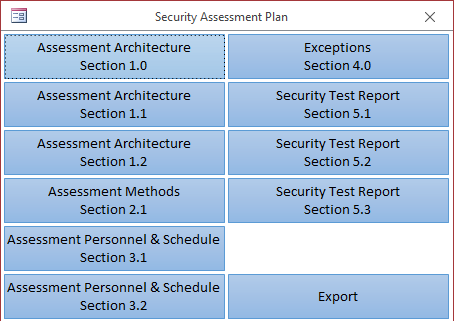
### Findings with Unselected Controls Report

Due to the requirement to add Security Controls associated with selected relevant STIGs, this report will show any Security Controls that have STIGs associated with them but the controls aren’t selected. The selection of STIGs/SRGs on the STIG/SRG Selection Form is a prerequisite for this report.



### Security Assessment Plan

The Security Assessment Plan (SAP) shows the information for the all the tabs of the SAP for import into the Navy SAP template. Each section of the SAP has its own button and its own tab when exporting to Excel.



#### Assessment Architecture – System Name – Section 1.0

Section 1.0 corresponds to Section 1.0 of the Assessment Architecture tab of the Navy RMF Security Assessment Plan (SAP). Only one row of information is required.



#### Assessment Architecture – Baseline Hardware List – Section 1.1

Section 1.1 corresponds to Section 1.1 of the Assessment Architecture tab of the Navy RMF Security Assessment Plan (SAP). 

#### Assessment Architecture – Baseline Software List – Section 1.2

Section 1.2 corresponds to Section 1.2 of the Assessment Architecture tab of the Navy RMF Security Assessment Plan (SAP). 

#### Assessment Methods – Requirements Traceability – Section 2.1

Section 2.1 corresponds to Section 2.1 of the Assessment Methods tab of the Navy RMF Security Assessment Plan (SAP). 

#### Assessment Personnel & Schedule – Assessment Personnel – Section 3.1

Section 3.1 corresponds to Section 3.1 of the Assessment Personnel & Schedule tab of the Navy RMF Security Assessment Plan (SAP). 

#### Assessment Personnel & Schedule – Assessment Schedule – Section 3.2

Section 3.2 corresponds to Section 3.2 of the Assessment Personnel & Schedule tab of the Navy RMF Security Assessment Plan (SAP). 

#### Exceptions – Exceptions in Testing – Section 4.0

Section 4.0 corresponds to Section 4.0 of the Exceptions tab of the Navy RMF Security Assessment Plan (SAP). Select Yes or No in the Dropdown field. If yes, replace the text in the Additional Information Required field.



#### Security Test Report – False Positives – Section 5.1

Section 5.1 corresponds to Section 5.1 of the Security Test Report tab of the Navy RMF Security Assessment Plan (SAP). 

#### Security Test Report – Misleading Reports – Section 5.2

Section 5.2 corresponds to Section 5.2 of the Security Test Report tab of the Navy RMF Security Assessment Plan (SAP). 

#### Security Test Report – Summary of Issue: Background – Section 5.3

Section 5.3 corresponds to Section 5.3 of the Security Test Report tab of the Navy RMF Security Assessment Plan (SAP). 

#### Security Assessment Plan – Export

The Export button will export all the previous sections to one Microsoft Excel spreadsheets with each section on a separate tab.



# Troubleshooting

## Windows

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

If a File not Found error occurs when opening the database, some references may be missing.

1. Click Database Tools 🡪 Visual Basic
2. In the Microsoft Visual Basic for Applications window, click Tools 🡪 References
3. You may need to select the Microsoft Excel xx.0 Object Library and/or Microsoft Office xx.0 Object Library
4. Click Ok.
5. Close Microsoft Visual Basic for Applications

\*\*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.

## Verify data is correct

When importing data, verify that the import data is correct.

## Compact and Repair

Compact and Repair the database routinely. Compact the back end database separately from the front end database only when the front end database is closed.

## Changing Data Issues

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.

## Database goes to code window when opening for the first time

This may be the result of a missing reference. Click the square stop button. Click Tools 🡪 References. If one of the references listed shows the text, Missing, uncheck it. You may have to close and reopen the database to get to the References.

## Error Updating Back End Database after installing new version

If a message box shows up when attempting to update the back end database after installing a new front end, take note of the record number appearing in the box. Open the back end database. Open the tbl\_Defaults table. Find the ubeVersion field and change the value to the one in the message box.

# How to create new build of SRP and post to GitHub

1. Update CCIs.
2. Copy files to C:\Scan Results Processor.
3. Open front end at new location.
4. Select back end database from new location.
   1. Click Select BackEnd.
   2. Edit text in Database Path field to match new location.
   3. After database reloads, verify path at top of MainGui.
5. On MainGui, click Setup.
6. On Setup form, click Clear Database.
7. Make sure that StatCounter On/Off is set to On.
8. Close and compact front end and back end databases.
9. Put all files in a zip file named Scan Results Processor - <version>.zip.
10. Run nullsoft scriptable install system (NSIS) application.
11. Click Installer based on ZIP file in Compiler section.
12. Open Source ZIP File.
13. Click Generate.
14. When script completes, click Close.
15. Close NSIS.
16. Open GitHub Desktop.
17. Go to the correct repository.
18. Click the open this repository in Explorer link.
19. Overwrite any files with new files, ie. Front end and back end databases, SRPCCIUpdate.csv, Manual. Do not move the .zip or .exe files.
20. The files changes will show in the Changes section of the Github Desktop.
21. Enter Summary text.
22. Click Commit to master.
23. After the files are committed, click Push origin.
24. Wait for Pushing to origin to complete.
25. Close GitHub Desktop.
26. Go to repository in github.com
27. Click the Releases link.
28. Click Draft a new release.
29. Enter the new version in the Tag Version field, preceded by “v”.
30. Enter a new title in the Release Title field, “Scan Results Processor – RMF v<version>.
31. Enter a release description in the Describe this Release field, 1st line – “Release Notes”, 2nd line – v<version. YYYYMMDD, 3rd line – blank, 4th line – copy/paste release notes from Manual.
32. Drag executable created by NSIS to Attach Binaries field.
33. Click Publish release.
34. Go to main repository page in github.com
35. Verify that files have updated.
36. Close github.com.
37. Go to folder with development database on computer.
38. Rename file names for development version of front end and back end databases to new version number.
39. Open new front end version.
40. On MainGui, click Select Backend.
41. Edit Database Name and Database Path to match new version number.
42. Double click Backend Database path.
43. Open Visual Basic code.
44. Open BackendUpdate1 Module.
45. Change value for New Version.
46. Close and Save Visual Basic code.
47. On MainGui, click Setup.
48. Change version number in Program Name – Title.
49. Exit database.

# Point 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.

## 1.0.0

* Initial Version

## 1.0.1

* Changed labels of Vulnerability and Non-Vulnerability fields to Non-Compliant Results and Compliant Results.
* Added ability to copy Actual Results field to Compliant Results field by double clicking on Actual Results label in Assessment Procedures Form.
* Removed Expected Results from Assessment Procedures Form.
* Added instructions text to Test By label on Assessment Procedures Form.
* Changed DoD Tier 1 Partial/Complete Inheritance text in Security Controls to DoD Tier 1 Hybrid/Common Control.

## 1.1.0

* Fixed query for Add Vulnerability to 800.53 Scan Results
* Updated buttons and Reports for Security Controls and Assessment Procedures and other forms
* Added double click functionality to FISMA Report Date field
* Added CyberSafe A and CyberSafe B to Overlay field on SAR
* Moved Classified Overlay to beginning of section 6 of SAR
* Updated truncated CCI Definition and Implementation Guidance Text
* Created RAR Sheet 1 that can be exported to RAR template and added as new sheet with sheet name the same as query name
* Disabled Inherited From field on Assessment Procedures form if CCI cannot be inherited
* Updated Assessment Procedures and Security Controls with DON Tier 2 Inheritance
* Added IAVM functionality
* Added Assessment Procedures view when clicking Security Control on Security Control Form
* Fixed Database open to default to Splash form

## 1.2.0

* Added Export to PDF button on Security Controls and Assessment Procedures Forms
* Added Export to Excel button on Security Controls and Assessment Procedures Forms
* Adjusted Double Click functionality on Assessment Procedures Form
* Added Tier 3 Inheritance
* Added ability to see if Overlays have been added by the color of the Overlay buttons on the Overlays form

## 1.2.1

* Added IAVM tables and Overlay fields to list of deleted items when clearing database
* Error checking applied to opening and closing forms
* Changed Import Location Form to automatically check for the STIG Viewer version

## 1.2.2

* Fixed Navigation Pane opening when importing STIG
* Fixed setting of Final Scan options when closing Scan Results Form
* Fixed sort on Scan Results Form and All Scan Results Form
* Fixed setting Plan when creating vulnerability from Assessment Procedures
* Fixed setting POAMStatus when creating vulnerability from Assessment Procedures
* AutoBackup added to Setup screen to allow for an auto backup of backend database when importing scans
* Added ability to filter for Applicable IAVMs on IAVM Project Report
* Fixed bug causing Navigation Pane to open when importing scans
* Added CVE field from ACAS SecurityCenter scans to Check Content field

## 1.2.3

* Fixed Assessment Procedures not listing correct findings in Vulnerabilities field
* Now checking for ACAS scan with no open findings
* Now updating ChecklistType in tbl\_Hosts, tbl\_ScanResults and tbl\_UniqueScanResults when Checklist Type is changed on the Scans Form
* Fixed Before Update on Plan drop down box on Scan Results and All Scan Results forms

## 1.2.4

* Fixed Before Update on Plan drop down box on Scan Results and All Scan Results forms
* Fixed Security Controls field on POA&M not having values unless going to Assessment Procedures Sub Form for each vulnerability in Scan Results Form

## 1.2.5

* Optimized updating Hosts when importing scans and creating vulnerabilities from Assessment Procedures
* General cleanup
* Changed length of CCI field in tbl\_AssessmentProcedures from 255 characters to 10
* Fixed sort order on Assessment Procedures Report

## 1.2.6

* Fixed Back End import from DIACAP functionality
* Added Overlay field to Security Controls Form
* Set Security Controls Designation field on Security Controls Form automatically based on Inherited From field
* Fixed incorrect characters in ID for Security Controls
* Added Actual Results field to Assessment Procedures subform on Security Controls Form
* Removed last comma and space from Overlay field in tbl\_800-53\_Controls

## 1.2.7

* Added Confidentiality, Integrity and Availability levels to bottom of Security Controls Form
* Fixed values in Overlays and Assessment Procedures table
  + AC-19(4) removed from Classified Overlay
  + SC-6 added to Cybersafe A Overlay
  + CCI-002714 added to SI-7(5) as DON Tier 2 Inherited
  + CCI-002715 added to SI-7(5) as not inherited
  + SI-7(5) marked as DON Tier 2 Hybrid Control

## 1.3.0

* Added Cat I, Cat II and Cat III buttons to populate Severity field on Assessment Procedures Form
* Adding Vulnerability now goes to next record on Assessment Procedures Form
* Widened left hand column of Assessment Procedures Form
* Added Overlay field to Assessment Procedures Form
* Added Confidentiality, Integrity and Availability levels to bottom of Assessment Procedures Form
* Fixed Confidentiality, Integrity and Availability levels at bottom of Assessment Procedures Form and Security Controls Form causing form to be not updateable
* Fixed All Scan Results Report on All Scan Results Form
* Changed title of combo box on MainGui to Select Scan
* Added STIG/SRG Form to select relevant STIGs/SRGs
* Added My STIGs and All STIGs buttons to CCI field on Assessment Procedures Form to show associated STIGs
* Added instructions to import CCIs from STIG Viewer Export and am now bundling spreadsheet with each release

## 1.3.1

* Add Checklist Type lists to Import Location Form
* Fixed VMSID field in tbl\_ScanResults and tbl\_UniqueScanResults being only 8 characters long instead of 20 when importing from DIACAP
* Updated Assessment Procedures Form to include filtering functionality when double clicking Inherited From label or Actual Results label
* Removed message box after adding vulnerability to scan results – it just goes to next record
* Changed functionality of My STIGs and All STIGs buttons on Assessment Procedures Form to be visible only when relevant
* Fixed Confidentiality, Integrity and Availability levels at bottom of Assessment Procedures Form and Security Controls Form causing value to be missing for “C” only, “I” only or “A” only
* Fixed Exporting to PDF of Assessment Procedures Form
* Added Updating in background when Updating Vulnerabilities on Assessment Procedures Form
* Fixed Compliance Status on Assessment Procedures Form when Updating Vulnerabilities
* STIG is marked as Selected in lst\_STIG table if it matches the Checklist Type entered on Import Location form when importing STIGs/SRGs
* Not Applicable field on Assessment Procedures Form automatically updates based on text or lack of text in Not Applicable Justification field
* Update column sizes on Assessment Procedures Form
* Double clicking the Control Number on the Assessment Procedures Form will bring up the related Security Control information

## 1.3.2

* Changed data type of many fields on Security Plan to Memo to accommodate more text
* Added About form to show current and latest releases with a link to download the latest version
* Database will now check to see if the current version matches the latest version; if not, a choice will be given to close the database and go to the web to download the latest version
* Updated copyright notices to automatically enter year and version
* Added table for IA TA Standards (no relationships, forms or reports yet)
* Updated tbl\_AssessmentProcedures with Tier 3 Inheritance
* Added error checking for no records on Assessment Procedures Form when filtering
* Added error checking on no Current Version
* Automatically update Current Version when opening database

## 1.3.3

* Fixed bug in IAVM form limiting import to 4000 records
* MainGui is restored automatically when previous screens are maximized
* When clicking Add as Vulnerability to Scan Results button on Assessment Procedures Form, the focus will go to the Control Number field
* Adjusting coloring of CIA at bottom of Assessment Procedures Form
* Added Double click for text to Control Number field on Assessment Procedures Form
* Fixed ACAS Nessus imports checking Severity field instead of Risk field
* Checklist Version drop down on Import Location form now shows Checklist versions for ACAS
* Added Title to Import Complete message box when importing scan

## 1.3.4

* Added CCIUpdateDate field in tbl\_Defaults to track last time the CCIs were updated
* Added update check to see if CCIs have been updated within the past six months.
* Updated CCI Import spreadsheet – STIG column empty
* Created report to show findings associated with unselected security controls
* Updated code on Update Vulnerabilities button to cycle through Non-Vulnerabilities before Vulnerabilities in order to make Severity value correct based on Vulnerabilities also no longer writing Severity for non-vulnerabilities
* Updated code on Update Vulnerabilities button on Assessment Procedures form to cycle through the InheritedFrom field to automatically populate the InheritedFrom, SecurityControlDesignation and ImplementationStatus fields on the Security Control form
* Updated eMASS Test Result Import to only show Assessment Procedures for Selected Security Controls
* Updated wrongly formatted ControlIDs in tbl\_Control\_Overlays (same Controls that were fixed in the tbl\_800-53\_Controls in version 1.2.6)
* Added missing Assessment Procedures: IA-1.10 (CCI-001932), IA-1.11 (CCI-001934), AC-2(8).1 (CCI-002138) and AC-2(8).2 (CCI-0032139)
* Removed limitation on InheritedFrom field on Assessment Procedures form
* Adjusted code for checking version number because Microsoft sucks (You will see a brief IE pop-up of the github web page
* Added fields to tbl\_IATAStandards
* Added combo box for Compliance in IATA Standards
* Added IATA Standards query pop-up when double-clicking CCI field on Assessment Procedures form
* Auto generating Inherited From values on Security Controls form based on Inherited From values on Assessment Procedures form
* Auto generating Not Applicable and Not Applicable Justification values on Security Controls form based on Not Applicable and Not Applicable Justification values on Assessment Procedures form
* Auto generating Implementation Status values on Security Controls form based on Inherited From and Not Applicable values on Assessment Procedures form
* Auto generating Security Control Designation values on Security Controls form based on Inherited From values on Assessment Procedures form
* Set Implementation Status to “Planned” for all Controls on Security Controls form on new and cleared database

## 1.3.5

* Updated code for About form
* Clear Compliance Status from IATA Standards when clearing database
* Added StatCounter field to tbl\_Defaults
* Added ability to track IP address using StatCounter website
* Added ability to opt out of StatCounter tracking by drop down box on Setup form
* Reimported CCI spreadsheet

## 1.3.6

* Created Hardware List form and report for SAP
* Added Manufacturer field to tbl\_Software
* Created Software List form and report for SAP
* Remove AC-18(5) from Classified Overlay
* Updated Implementation Guidance and Assessment Procedures text for AC-20(2).1
* Add frm\_SAP to track various sections of Security Assessment Plan
* Added buttons to frm\_SAP to enter data on forms associated with various sections of the SAP
* Added Export button to export data on forms associated with various sections of the SAP to a Microsoft Excel spreadsheet
* Add tbl\_SAP\_Traceability and associated forms, queries and reports to track Section 2.1 of Security Assessment Plan
* Add tbl\_SAP\_Personnel and associated forms, queries and reports to track Section 3.1 of Security Assessment Plan
* Add tbl\_SAP\_Schedule and associated forms, queries and reports to track Section 3.2 of Security Assessment Plan
* Add tbl\_SAP\_Exceptions and associated forms, queries and reports to track Section 4.0 of Security Assessment Plan
* Add tbl\_SAP\_FalsePositives and associated forms, queries and reports to track Section 5.1 of Security Assessment Plan
* Add tbl\_SAP\_MisleadingReports and associated forms, queries and reports to track Section 5.2 of Security Assessment Plan
* Add tbl\_SAP\_Summary and associated forms, queries and reports to track Section 5.3 of Security Assessment Plan
* Added SAP data to Clear functionality on Setup page

## 1.3.7

* Added new fields to Security Plan based on changes to eMASS
* Fixed problem with previous spreadsheet not being killed on SAP exports
* Added Monitored Control Information to Security Controls for input to System Level Continuous Monitoring Plan
* Added Monitored field to Security Controls Form
* Automatically change Monitored to No when changing Not Applicable to Yes
* Automatically change Monitored to nothing when changing Not Applicable to No
* Double-click Monitored label opens Monitored Control Information Form
* Added ability to export all monitored control information to spreadsheet

## 1.3.8

* Added Unmonitored Control Information to Security Controls and Navy SLCM Strategy Controls Table form
* Automatically set Monitored to No when associated with Control Criticality diamond in eMASS (Red, Yellow, White)
* Automatically set Control Criticality and ASR Distribution when clearing database based on values of Control Criticality in eMASS
* Renamed Monitored Controls form to Navy SLCM Strategy Controls Table to match template
* Updated Navy SLCM Strategy Controls Table export spreadsheet to include Unmonitored Controls tab

## 1.3.9

* Forced Save Record when changing Continuous Monitoring information
* Monitored Control fields are enabled/disabled based on values in Allocation Monitoring Method and Enhanced Monitoring Method fields
* Unmonitored Control fields are enabled/disabled based on value in Monitored field
* Allocation field on Continuous monitoring form is automatically generated based on Inherited From field when clicking Update Vulnerabilities on Assessment Procedures form
* Fixed Procedure Paint Button to On/Off text field
* Automatically copy Not Applicable Justification to Actual Results on Assessment Procedures form for Not Applicable Assessment Procedures
* Changed Not Applicable field on Assessment Procedures form to drop down box
* Added Last Updated field to tbl\_Defaults and MainGUI to show the last time that the database was updated
* Code added to most forms to update the Last Updated field when data is changed

## 1.3.10

* When linking CCIs to Vulnerabilities on Scan Results Form – now deleting record associated with vulnerability before adding it back into tbl\_VulnID\_800.53Controls
* When selecting POA&M Import or RAR Reports, a warning will pop up if there are open findings without associated CCIs
* Updated POA&M Import queries to match latest version of eMASS POA&M Import Template
* Added to Scan Results Import queries to put ACAS Plugin ID into Rule ID field
* Changed combo box values for Frequency and Method on Continuous Monitoring form to match values in eMASS Implementation Plan
* Added Reporting, Tracking and SLCM Comments field to Continuous Monitoring form
* Updated Implementation Plan query to match eMASS Implementation Plan
* Added CCI-000057 (AC-11.4) to Assessment Procedures table (missing in eMASS and Knowledge Service)
* Changing Splash screen picture to something less appropriate
* Performed IAVM Import

## 1.3.11

* Changed qry\_Update\_ControlCriticality to mark all Red, Yellow and White controls as Monitored = Yes and all others = No
* More updates to Continuous Monitoring form
* Updates to tbl\_800-53\_Controls\_Criticality

## 1.3.12

* Changes from v.1.3.9 were lost, so they have been put back
* Updated code to update SRP Last Update date
* Updated code for Procedure Paint On/Off

## 1.3.13

* Updated color of SRPLastUpdate field on MainGui based on background color
* Updated CCI update to truncate STIG/SRG names prior to “ :: “ characters
* Fixed Warnings turning back on when changing Plan on Scan Results and All Scan Results forms
* Updated query for All Open Scan Results report
* Increased size of RMF Activity field on Security Plan form
* Updated code on Report Selection to force Count of findings with no associated controls to be zero
* Fix code break when checking latest version from github.com
* Updated qry\_SecurityControls to include SLCMReporting, SLCMTracking and SLCMComments fields
* Updated Warnings turning back on after form update when saving record
* Fixed Data Sheet view of Assessment Procedures form to decrease width of CCI field
* Updated All Scan Results Report to not show duplicates
* Updated Scan Summary form sort order
* Added SortNo field to tables, queries and forms for Hardware, Software, PPS and Test Plan
* Added Inherited From field to Inheritance List Report
* Added Checklist Type to Mitigated Vulnerabilities Report
* Added Year 1, Year 2 and Year 3 to FISMA table, query, form and report
* Updated FISMA form and report by adding Hybrid, Year 1, Year 2 and Year 3 fields and other changes to labels and formatting
* Updated Navy SLCM Strategy Controls form to allow entries for Year 1, Year 2 and Year 3 testing of controls
* FISMA Year 1, 2 and 3 check boxes are automatically checked when the Update Vulnerabilities button is clicked on the Assessment Procedures form for automated results
* FISMA Year 1, 2 and 3 check boxes are cleared by clicking the Clear FISMA Year button on the Security Controls form
* Updated SAP forms with Sort Number column
* Updated imports to update ScanID for ALL findings instead of just changed findings in tbl\_UniqueScanResults

## 1.4.0

* Updated call to github.com when opening database
* Changed Message Box Title if a newer version is available
* Changed Default button to No on Message Box if a newer version is available
* Updated Excel calls (exports) throughout to add a Kill of original spreadsheet after it is copied to one with a longer name
* Updated query for Inheritance Report
* Added page numbers to Inheritance Report
* Updated query for CCI Import to truncate STIG name correctly

## 1.4.1

* Increased size of ChecklistType field in tbl\_Scans to 100
* Updated CCI Import to truncate STIG name correctly
* Removed trailing spaces from lst\_STIG and tbl\_VulnID\_STIG tables
* Changed code for Update Vulnerabilities button on Assessment Procedures form to pull in NoVulnerabilities if InheritedFrom field is not blank
* Fix InheritedFrom text for IA-1.10 and IA-1.11
* Update qry\_Hosts\_Open to be limited to only the latest scan for each Checklist so the source field (Hosts) in the POA&M will show correctly
* CCI update based on 7/2018 STIG compilation

## 1.4.2

* Modified a query used when updating CCIs
* Add filterable but non-editable Baselined checkbox on Scan Results and All Scan Results forms
* Removed Report capability from SAP forms for all except Hardware and Software
* Fixed code for SAP Software Report to point to correct report and query names
* Removed conditional formatting from SAP Hardware and Software Reports
* Doubled height of PPS List fields
* Change field type of Purpose field in Software Table to Memo to allow more than 256 characters
* Fixed tab order for Software List form
* Increase field size of Acronym field in Software Table to 50
* Added Executive Summary field to Security Plan
* Update of Title field on Scan Results form and All Scan Results form now updates tbl\_UniqueScan Results table
* Update Executive Summary in Security Plan when clearing database
* Added testable field to tbl\_Software
* Software form in SAP pulls in software from tbl\_Software if testable is Y
* Updated Implementation Plan query to match export from eMASS
* Changed CommonControlProvider field on Continuous Monitoring form to drop down box with limited, auto-generated values of “DoD”, “Component” or “Enclave” based on Inherited From value
* Updated code to check for latest version to take into account that github.com is moving text around
* Switch CCI numbers for Assessment Procedures AC-6(7).4 and AC-19(5).1 due to mismatch between IATA standards Security Control Selection Spreadsheet and eMASS/IASE CCI list
* Switch CCI numbers for Assessment Procedures IA-5.11 and IA-5(5).1 due to mismatch between IATA standards Security Control Selection Spreadsheet and eMASS/IASE CCI list
* Severity, Relevance, Likelihood, Impact and Residual Risk fields have been added to the Security Controls form; their content is generated from the highest value of ongoing findings associated with each Security Control
* The contents of the Vulnerability summary, Impact Description and Recommendations fields, which have been added to the Security Controls form, are concatenations of all the values from ongoing findings associated with each Security Control
* The values for the Severity, Relevance, Likelihood, Impact, Residual Risk, Vulnerability Summary, Impact Description and Recommendations fields, on the Security Controls form, are generated by clicking the Update Vulnerabilities button on the Assessment Procedures form
* Updated Status field of eMASS POA&M Import (Closed Findings Since Baseline) to include the Date Completed