



Fast-Tracking the Approval of Mission- Critical Software for Use on the AFNet

MSgt Justin Schoenthal



August 2018

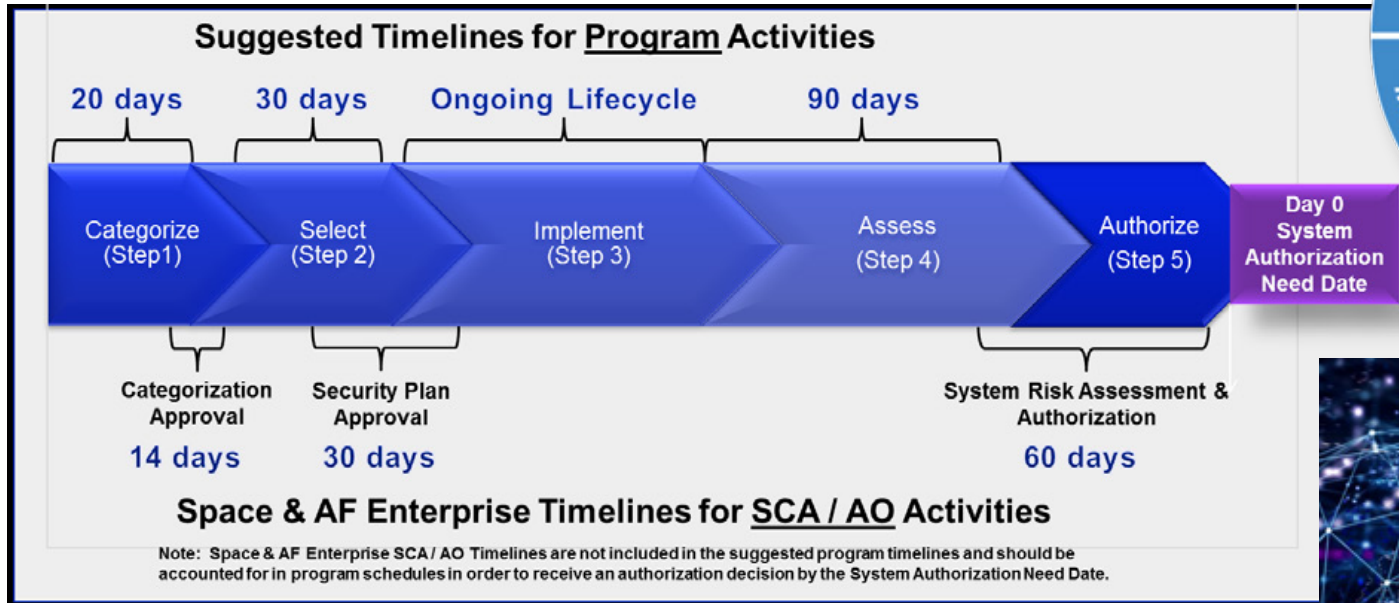
UNCLASSIFIED

- **What is SACA**
- **Software Assessment Methods**
- **Assessment Process**
- **Our Test Process**
 - **Desktop/Server**
 - **Web Application**
 - **Mobile**
- **Impact**
- **How to Submit a Request**



- **We assess Desktop, Server, Web, and Mobile software applications per AFI 17-101**
- **We check for security, supportability, and compatibility within AFNIC's Realistic AFNET Validation Environment (RAVE)**
- **We identify mitigations to support the AFNET Security Control Assessor (SCA) for certifying low-risk software to be used throughout the Air Force**
- **We team with the AFNET Authorizing Official (AO) as well as other AOs**

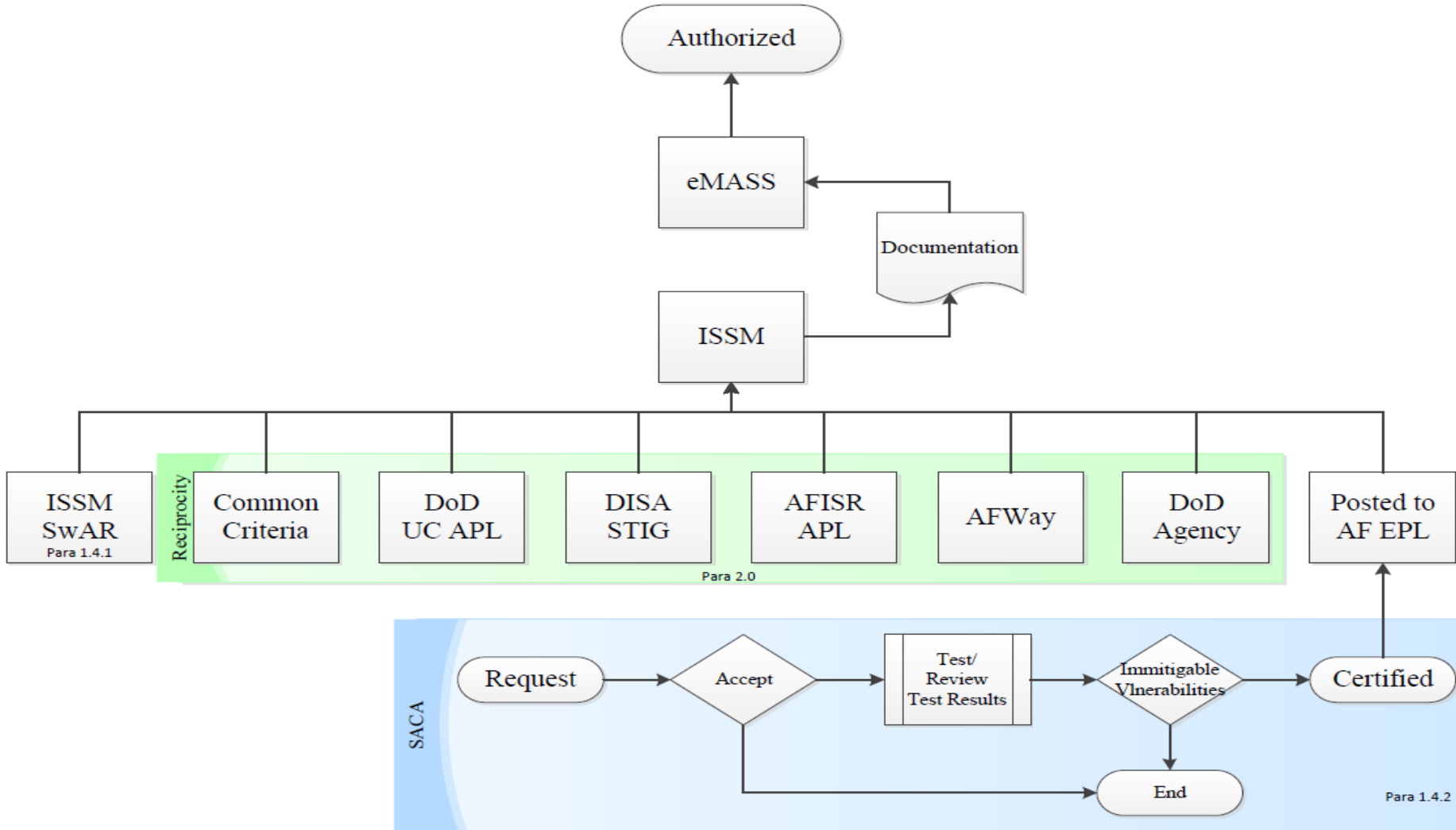
- **Two formal avenues for gaining approval to use mission-required software**
- **RMF Enclave Package (A&A)**



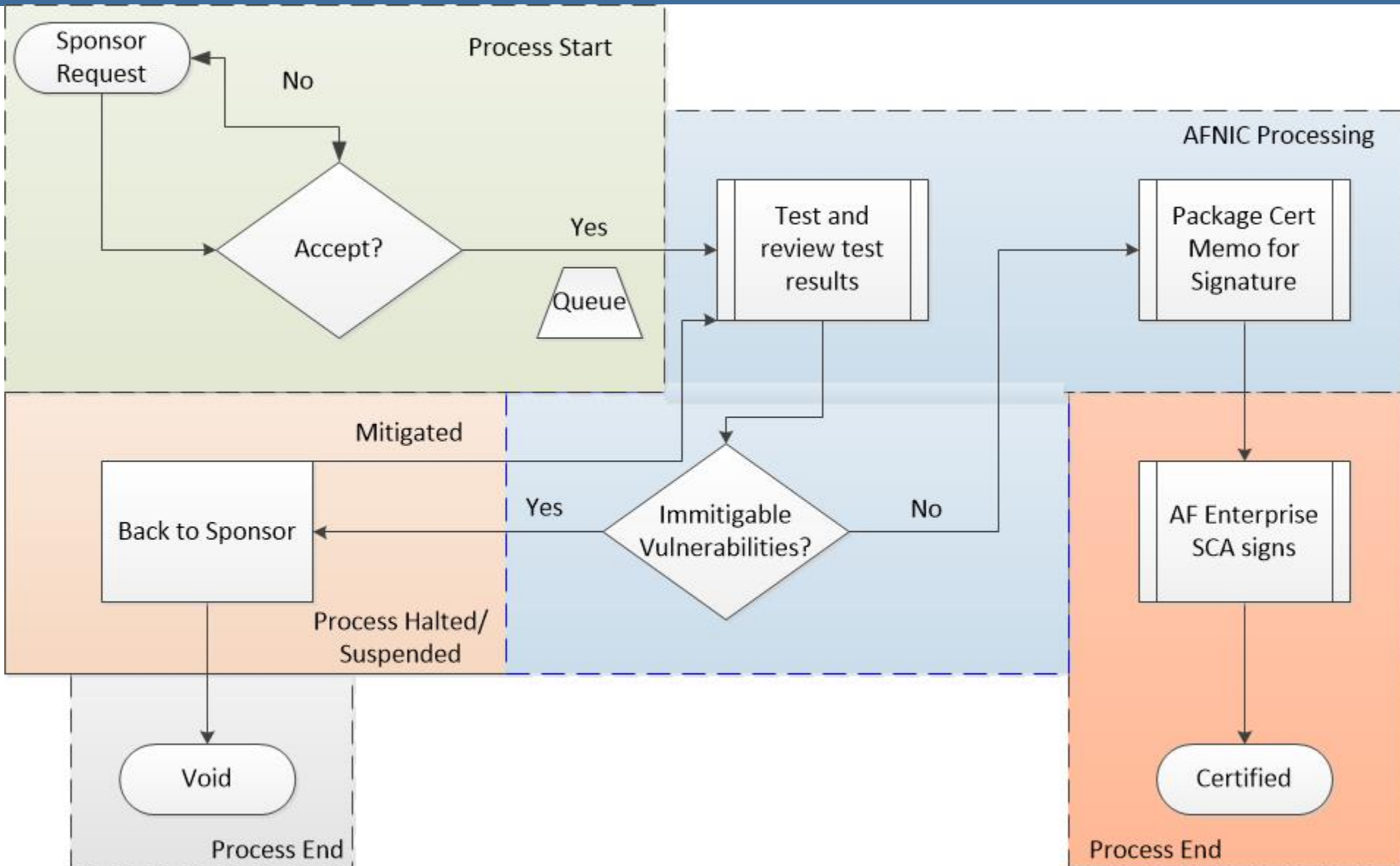
- **Assess Only (aka AF SACA)**
 - **One stop shopping at AFNIC**
 - **Easy to contact**
 - **Easy to browse certified products**
 - **Easy to request**
 - **Free**
 - **Trusted**
 - **Continually improving processes**

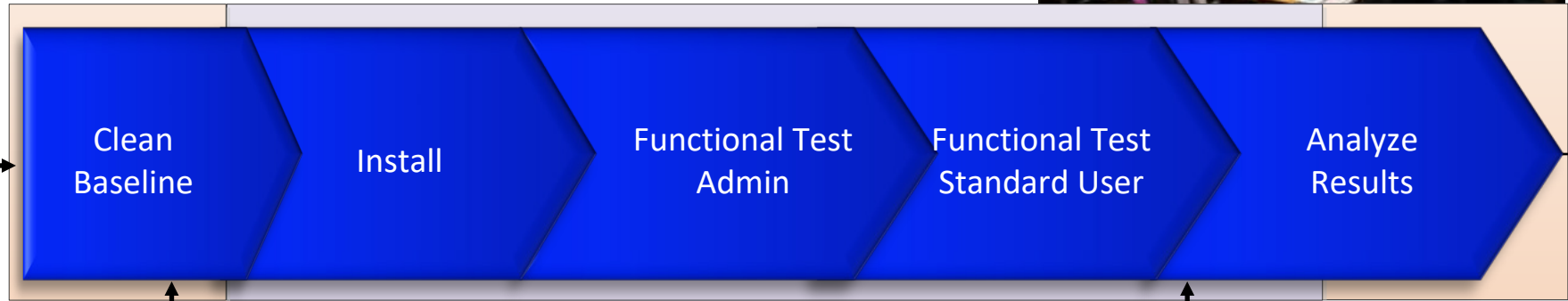


- **Software Products Excluded from AF SACA**
 - Products whose main function is encryption, but does **NOT** have FIPS 140-2 certification
 - Software that does **NOT** have a vendor or sponsor responsible for developing security patches
 - Software with immitigable Moderate (CAT II) or higher vulnerabilities
 - Software that uses ports, protocols, or services **NOT** listed in the DoD Category Assurance List (CAL)
 - Unsupported freeware and shareware
 - Open Source Software (OSS) with **NO** configuration/software support plan
 - IA or IA-enabled products/software (IAW CNSSP No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products*)



IAW AFI 17-101, Atch 2 - ways 3rd party software products and applications get authorized for the network





Mkruntest

Packet Capture

Packet Capture

Mkruntest

Setup

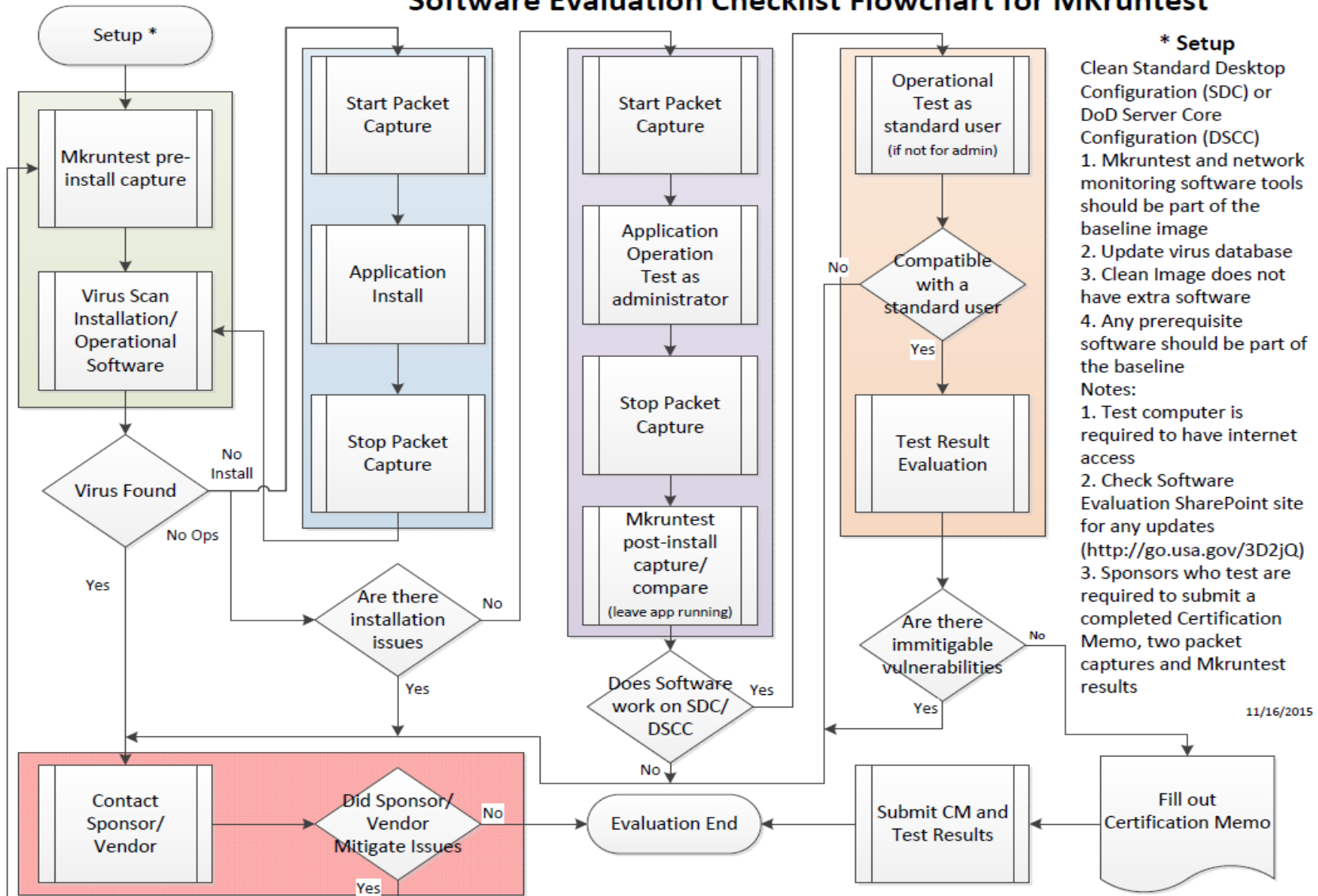
Clean Standard Desktop Configuration (SDC)/DoD Server Core Configuration (DSCC)

1. Mkruntest and packet capture tools should be part of the baseline
2. Update Virus Database
3. Internet Access required



Low Risk to the network?

Software Evaluation Checklist Flowchart for MKruntest



*** Setup**

- Clean Standard Desktop Configuration (SDC) or DoD Server Core Configuration (DSCC)
- 1. Mkruntest and network monitoring software tools should be part of the baseline image
- 2. Update virus database
- 3. Clean Image does not have extra software
- 4. Any prerequisite software should be part of the baseline

Notes:

- 1. Test computer is required to have internet access
- 2. Check Software Evaluation SharePoint site for any updates (<http://go.usa.gov/3D2jQ>)
- 3. Sponsors who test are required to submit a completed Certification Memo, two packet captures and Mkruntest results

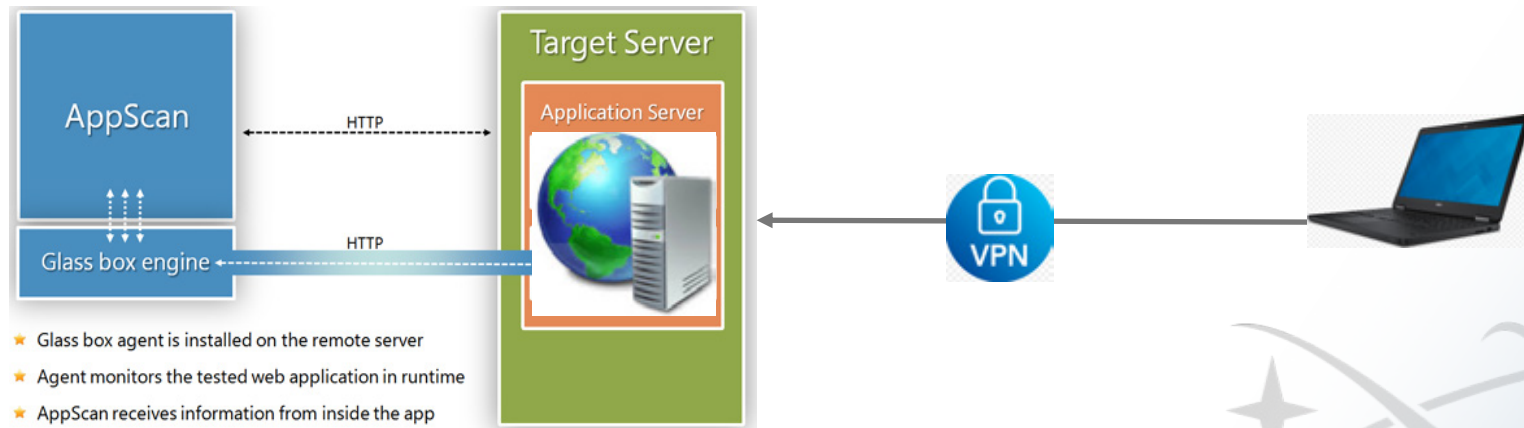
11/16/2015

Added Executables Report

Folder/File	File Version	Description
c:\program files (x86)\simoo_r3_mv5_w64\bin\simc.exe		
c:\program files (x86)\simoo_r3_mv5_w64\bin\simtran.exe		
c:\program files (x86)\simoo_r3_mv5_w64\bin\simxref.exe		
c:\program files (x86)\simoo_r3_mv5_w64\jre\bin\java-rmi.exe	7.0.50.5	Java(TM) Platform SE binary
c:\program files (x86)\simoo_r3_mv5_w64\jre\bin\java.exe	7.0.50.5	Java(TM) Platform SE binary
c:\program files (x86)\simoo_r3_mv5_w64\jre\bin\javacpl.exe	10.5.0.05	Java(TM) Control Panel
c:\program files (x86)\simoo_r3_mv5_w64\jre\bin\javaw.exe	7.0.50.5	Java(TM) Platform SE binary
c:\program files (x86)\simoo_r3_mv5_w64\jre\bin\javaws.exe	10.5.0.05	Java(TM) Web Start Launcher
c:\program files (x86)\simoo_r3_mv5_w64\jre\bin\jp2launcher.exe	10.5.0.05	Java(TM) Platform SE binary
c:\program files (x86)\simoo_r3_mv5_w64\jre\bin\keytool.exe	7.0.50.5	Java(TM) Platform SE binary
c:\program files (x86)\ibm\notes\lasr.dll	Build 20130120	KeyView Lotus Amipro 4.0 speed reader
c:\program files (x86)\ibm\notes\libeay32.dll	1.0.0c	OpenSSL Shared Library
c:\program files (x86)\ibm\notes\libpff.dll	20110413	Library to support the Personal Folder File (OST, PAB and PST) format
c:\program files (x86)\ibm\notes\libpng15.dll	1.5.12	PNG image compression library
c:\program files (x86)\ibm\notes\libz.dll	2.0.10.0	zlib data compression library
c:\program files (x86)\ibm\notes\z\zsr.dll	Build 20120519	KeyView Extract Library
c:\program files (x86)\ibm\notes\zlib1.dll	1.2.3	zlib data compression library
c:\program files (x86)\ibm\notes\c\icc\icclib\icclib.dll	1.4.5.0	IBM Crypto for C-language
c:\program files (x86)\ibm\notes\c\icc\icclib\icclib080.dll		
c:\program files (x86)\ibm\notes\c\icc\osslib\libeay32.dll	1.4.5.0	OpenSSL 0.9.7c 30 Sep 2003
c:\program files (x86)\ibm\notes\c\icc\osslib\libeay32ibm080.dll	8.0.0.0	OpenSSL Shared Library 0.98e
c:\program files (x86)\ibm\notes\framework\brokerbridge85\sthelper.dll	8.5.2.20130926.0645	Common Components for Microsoft Integration
c:\program files (x86)\ibm\notes\framework\brokerbridge85\sthelpeventmessage.dll		
c:\program files (x86)\ibm\notes\framework\brokerbridge85\sthelperx64.dll	8.5.2.20130926.0645	Common Components for Microsoft Integration

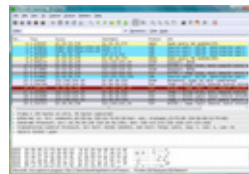
- **Web Application Evaluations**

- AFNIC uses AppScan
- If sponsor is testing--check for updates to AppScan prior to testing

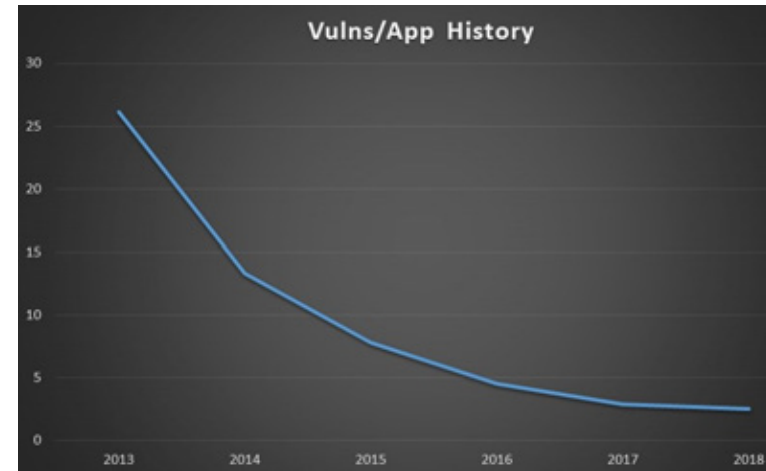


- **Success Example:** Base Visit Control Support System

- **Mobile Applications**
 - Currently iOS only
 - AFNIC performs packet captures



- **Comprehensive support**
 - **380 Application Requests**
 - **202 Certifications**
 - **646 Vulnerabilities Mitigated**



- The AF Evaluated Products List has over **1,000 certified products** as a first-stop shop

The Air Force doesn't operate without software, and software isn't certified for use without us

- **Desktop/Server Request**
 - Submit Application Request Worksheet ([ARW](#)) to AFNIC
 - Sponsor test in own environment-send to AFNIC
 - Sponsor can request access to AFNIC Realistic AFNET Validation Environment (RAVE) via [RAVE User Agreement](#)
- **AFNIC Web Application Request**
 - Submit completed and digitally signed [ARW](#) as sponsor tested in section 4
 - Submit [RAVE User Agreement](#), Installation Guide, System/Network Topology (SV-2) and Sponsor (not vendor) developed Application Systems Requirements documents
- **Mobile Application Request**
 - Complete the Mobile Application Request Worksheet ([MARW](#))

- **Contact Info**

- Bruce Betker, GS-13 (618) 229-6301 (DSN)779
- David Monson, GS-12 (618) 229-6482 (DSN)779
- Justin Schoenthal, MSgt (618) 229-6618 (DSN)779

- **Evaluated Products List**

- <https://cs2.eis.af.mil/sites/10336/Lists/COTSGOTS%20Software/EPL.aspx>





SERVITIO *75* **DEDICATI**
Years

- **Reciprocity Overview**

- <https://go.usa.gov/xN5KS>
- **For products not already assessed via the RMF or the AF SACA process, the Enterprise AO allows ISSMs to use software products that are certified by another DoD AO or SCA**
 - **Not as simple as it may sound...**



- **Who makes this happen?**

- **ISSM Role**

- Software products are considered assessed and require no additional formal test or evaluation, **so long as the actual environment, use, and configuration aligns with the intended environment, use, and configuration documented in the assessment package**
- The software product and **major version is verified** on one of the recognized sources:
 - *AF Evaluated Products List (SACA)*
 - *National Information Assurance Partnership*
 - DoD Unified Capabilities
 - *DISA DoD/AF Enterprise Mobile App Store*
 - DISA STIG
 - *AF Intel Community Approved Products List*
 - *AFWay*
 - *Army Networthiness*
- Prior to implementation, **ISSM must implement required mitigations**
- ISSM must update RMF documentation
 - This update will be considered a no security impact modification