U.S. AIR FORCE

eTools Lite System v1.9

SYSTEM SECURITY PLAN (SSP)

October 2020

Change Log

This record shall be maintained throughout the life of the document. Each change and published update shall be recorded.

CHANGE / REVISION RECORD			
Date	Description of Change	Affected Chapters	Made By:
5 February 2014	Update for iOS 7	Multiple	AF/A4PS
21 February 2014	Update for iOS 7 STIG	Multiple	AF/A4PS
19 March 2014	Update per updated guidance	Multiple	AF/A4PS
21 March 2014	Update per updated guidance	Multiple	AF/A4PS
26 March 2014	Update for APL memo, system name	Multiple	AF/A4PS
31 March 2014	Update the topology	Multiple	AF/A4PS
4 April 2014	Authorized User Agreement, user roles and responsibilities	Multiple	AF/A4PS
22 April 2014	Change to implementation to implementation guide	Multiple	AF/A4PS
7 May 2014	Included DD2875		AF/A4PS
12 May 2014	Revised password change guidance Deletion of DD2875	Multiple	AF/A4PS
23 May 2014	Revised per DAA-R comments	Multiple	AF/A4PS
02 Oct 2014	Updated to include security configuration changes resulting from the implementation of iOS 8.x. Change was determined to have No Security Impact (NSI) to the eTools Lite solution, so the SSP signature remains valid per the A4/7 Functional System's System Security Plan Guidance V8, August	Multiple	AF/A4PS

	2014.		
10 Oct 2014	Updated DISA IA Training web link and corrected eTools Lite version in Priv. User Agreement	Multiple	AF/A4PS
15 Oct 2014	Updated the User Permission matrix with system engineer; the addition of foreign nationals content for FOUO and other information	Multiple	AF/A4PS
20 Jan 2015	Updated to adhere to current SSP guidance	Multiple	AF/A4PA
09 Mar 2015	Fixed typo on screen lock timeout; added section 4.1.14; added airplane mode requirement prior to USB connection to cart	4.1.14	AF/A4PA
02 Apr 2015	Updated MacBook screenlock timeout to 15 minutes per STIG guidance; passwords chages set to 60 days	Multiple	AF/A4PA
11 May 2015	Updated to fix eTO refresh period following deployment; removed LIMS references	Multiple	AF/A4PA
23 Jul 2015	Updated to allow TAS for device management	4.1.8	AF/A4PA
04 Aug 2015	Updated to remove legacy configuration restrictions	Multiple	AF/A4PA
15 Sep 2016	Updated for eTools Lite v1.5	Multiple	AF/A4PA
28 Feb 2017	Updated for RMF Baseline	Multiple	AF/A4PA
28 Nov 2017	Configuration Change / priority 1 RMF control testing	Multiple	AF/A4PA
09 Jul 2018	Updated references to current AFMAN publications	Multiple	AF/A4PA
21 Sep 2018	Updated for eTools Lite v1.7	Multiple	AF/A4PA

01 May 2019	Create new section for Media Sanitization to comply with AFMAN 17-1301 para 6.2 and NIST SP 800-88.	5	AF/A4PA
08 Aug 2019	Adjusted the Authorized User Agreement to be an embedded pdf document	11 – Appendix B	AF/A4PA
10 Aug 2019	Updated the training policy to link to training URL's located at the new DISA Cyber.mil website.	Multiple	AF/A4PA
14 Aug 2019	Added a domain whitelist policy for deployments that are Cellular or Wi-Fi enabled and have an MDM with a domain whitelisting feature.	1.1.7.6. Whitelist Policy	AF/A4PA
14 Aug 2019	Added section on older generation iOS Devices that are no longer supported by Apple	3.1.11.2 Older generation iOS Devices that are no longer supported by Apple	AF/A4PA
16 Aug 2019	Added section 8 "Audit Review, Analysis, and Reporting" and Appendix D "Template for Bi-Annual Audit Assessments"	Multiple	AF/A4PA
09 Sep 2019	Removed the requirement to retain MacBook audit logs for one year before disposal since network connectivy and automation of log management is not currently available. Adjusted to be in compliance with MacOS STIG item AOSX-14-001029.	3.1.11.4 Standard eTools Lite MacBooks	AF/A4PA
25 Sep 2019	Added Information AssuranceVulnerablity Management (IAVM) process flow	3.1.10 System Configuration Management	AF/A4PA
26 Sep 2019	Added additional section for eTools Lite Technical Support.	9 Technical Support	AF/A4PA

10 Oct 2019	Added URL for EIS SharePoint site documentation on HERO devices	1.2 System Environment	AF/A4PA
18 Oct 2019	Added section for MiFi hotspots	1.1.7.2**Error! Reference source not found.** MiFi	AF/A4PA
11 Nov 2019	Adjusted verbiage to further clarify allowed connectivity and types of multifactor authentication.	1.1.7.10 Approved DoD Multifactor Authentication	AF/A4PA
11 Nov 2019	Adjusted verbiage to more granularly define network security for iOS and MacOS devices.	3.1.9 Network Security	AF/A4PA
12 DEC 2019	-Remove inaccurate statement which declared that Purebred requires an MDM. -Added Appendexes 16, 17, and 18.	multiple	AF/A4PA
10 FEB 2020	Updated the Authorized User Agreement to contain clause about negligence of due care in physical treatment of devices.	Appendix B	AF/A4PA
21 FEB 2020	Adjusted policy, guidance, and topology to remove references to now obsolete EMAS (middleware product from Monkton used in BRICE 1.0)	multiple	AF/A4PA
21 FEB 2020	Adusted to references to point to the AFTOFST SharePoint instead of the now defunct ELMS SharePoint	Multiple	AF/A4PA
06 MAR 2020	Updated system architecture diagram to reflect removal of EMAS and BRICE 1.0	Section 1	AF/A4PA
14 MAR 2020	Update policy and verbiage for Electronic Hard Drive to include references to STIGs, Air Force Policy, and User Agreement	multiple	AF/A4PA

27 MAR 2020	AFMAN 17-1201 is expired and out of cirulation. For physical security, replace references to AFMAN 17-1201 with referencs to AFMAN 17-1203 and AFMAN 17-1301.	multiple	AF/A4PA
30 MAR 2020	DoDI 5200.48 cancels DoDM 5200.01	multiple	AF/A4PA
30 MAR 2020	Added section 1.3.1 “Acquisition”	1.3.1	AF/A4PA
02 JUN 2020	1. Removed embedded objects and instead have hyperlinks to them on the AFTOFST SharePoint. 2. Correct typos where User Rules of Behavior was incorrectly being stated as being a different document from AF Form 4433.	Multiple	AF/A4PA
11 JUN 2020	Added section for Incident Response	Section 10	AF/A4PA
24 OCT 2020	Update for iOS 14	Multiple	AF/A4PA

Brigadier General Kathryn J. Johnson
A4/7 Designated Accrediting Authority

9 June 2014
Date

Mr. Eugene Collins
Functional Mission Owner
HQ A4L

13 JUN 2014
Date

Mr. Ken Morgan
Commercial Mobile Technology Lead
HQ A4ID

13 Jun 2014
Date

Table of Contents

1. System Description 12
1.1. System Functions and Capabilities 13
1.1.1. User Safeguards 13
1.1.2. Applications for eTools Lite devices 13
1.1.3. Battery Life 13
1.1.4. Screen Covers 13
1.1.5. Protective Cases 13
1.1.6. Deployment Support 13
1.1.6.1. Deploying eTOs with iOS Devices 14
1.1.6.2. Deploying with eTools Lite Components 14
1.1.7. Connectivity 14
1.1.7.1. Wi-Fi 14
1.1.7.2. MiFi 14
1.1.7.3. Cellular 14
1.1.7.4. Bluetooth Headsets 14
1.1.7.5. BlueDriver On-Board Diagnostics II (OBDII) Connector 15
1.1.7.6. Mobile Device Management / Mobile Content Management 15
1.1.7.7. Internet Domain Whitelist Policy 15
1.1.7.8. Device-to-device Communications 15
1.1.7.9. Approved DoD Multifactor Authentication 16
1.1.8. eTools Lite Architecture 16
1.1.9. System Resources 16
1.1.10. FOUO Information Currency 16
1.1.10.1. eTO Currency 16
1.2. System Environment 17
1.3. Description of Hardware and Software 17
1.3.1. Acquisition 17
1.3.2. iOS Devices 17
1.3.3. MacBooks 17
1.3.4. External Hard Drive (EHD) 18
1.3.5. Standard Desktop Configuration (SDC) Computers 19
1.3.6. Approved Software / Hardware 19
1.4. Supported Mission 19
1.5. Data Types / Protection Methods 19
1.6. System Availability 20
1.7. Backup and Recovery 20
1.8. Supporting Documentation 20

2. System Topology 22

2.1. System Interfaces... 22

3. Users, Locations, and End Point Devices... 22

3.1.1. System Access Rules & Policy... 23
3.1.2. Account Management.. 23
3.1.3. User Permission Matrix 24
3.1.4. Foreign Nationals 25
3.1.5. Access to eTools Lite 25
3.1.6. User Rules of Behavior 25
3.1.6.1. Additional User Agreement Guidelines 26
3.1.7. Failure to follow User Rules of Behavior or Authorized User Agreement........ 26
3.1.8. Physical Security 26
3.1.8.1. Hardware Accountability... 27
3.1.9. Network Security... 28
3.1.10. System Configuration Management 28
3.1.11. Device Configuration Policy 29
3.1.11.1. iOS Devices 29
3.1.11.2. Mac OS Devices 30
3.1.12. iCloud / Online File Sharing... 30
3.1.13. Remote Access 30

4. Authorized User Training Requirements.. 30

5. Media Sanitization and Physical Breakage/Damage 31

5.1. Media Sanitization.. 31
5.2. Repairs.. 31
5.3. Re-Provisioning 31

6. Policy & Procedures Overview for eTools Lite Users 31

6.1. MAJCOM... 31
6.2. Group Commander or Equivalent 32
6.3. Authorized User.. 32
6.3.1. Additional Authorized Users Program Support 33
6.3.2. Assistant Authorized Users 33
6.4. Device Custodian.. 33
6.5. Standard User 33

7. Security Funding Strategy.. 34

8. Audit Review, Analysis, and Reporting.. 34

9. Technical Support 34

10. System Identification Profile (SIP) 35

11. Plan of Actions and Milestones (POA&M) 35

12. Policy (AF, DoD) 35

13. References and Resources 36

FIGURES

Figure 1: eTools Lite Architecture 22

Figure 2: Process Flow for Vulnerability Alerts and Security Patches 29

Figure 3: Process Flow for Technical Support 34

TABLES

Table 1: System Identification 10

Table 2: eTools Lite Key IA Roles 11

Table 3: User Permission Matrix 24

Table 1: System Identification

System Name	eTools Lite v1.9
System Acronym	eTools Lite
Confidentiality Impact	LOW
Integrity Impact	LOW
Availability Impact	LOW
Information System Security Manager (ISSM)	Ms. Janina Green, AF/A4PA janina.l.green.ctr@us.af.mil Commercial: 410.382.8860
Air Staff Functional Sponsor	Theresa Moore, AF/A4PA theresa.a.moore47@us.af.mil DSN: 612-4160; Commercial: 240.612.4160
Functional Mission Owner	Mr. Eugene Collins, AF/A4L Eugene.collins18.civ@mail.mil DSN: 225-4900; Commercial: 703.695.4900
Functional Mission Owner	MSgt Robin McGill ANG NGB/A4MM robin.r.mcgill.mil@mail.mil DSN: 612-8122; Commercial: 240.612.8122
Functional Mission Owner	MSgt Jordan Miles ANG NGB A2/3/6 jordan.a.miles4.mil@mail.mil DSN: 612-9235; Commercial: 240.612.9235
Information Systems Owner	Theresa Moore, AF/A4P theresa.a.moore47@us.af.mil DSN 612-4160; Commercial: 703.612-4160
Authorizing Official (AO)	Brigadier General Darren Cole, AF/A4P darren.cole@us.af.mil DSN 612-4179; Commercial: 703.612.4179
Security Control Assessor	James Morris, AF/A4P James.morris.ctr@us.af.mil Commercial: 334-416-7045

NOTE: Supporting material referenced in this document can be obtained from the AF/A4 Enterprise Logistics Mobile Services (ELMS) Project Office.

Security Appointments

The following table lists the eTools Lite device key IA roles and personnel:

Table 2: eTools Lite Key IA Roles

Role	Name	Organization	E-mail	Phone
AO	BG Darren Cole	AF/A4P	darren.cole@us.af.mil	DSN 227-2822
AOD-R	Mr. Carlo Deguzman	AF/A4PA	carlo.deguzman.ctr@us.af.mil	(240) 612-4179
SCA	Mr. William Kramer	AFLCMC/H NIZ	william.kramer.5@us.af.mil	(334) 416-4553
SCAR	Mr. James Morris	AFLCMC/HI QC	James.morris.47.ctr@us.af.mil	(312) 596-7045
System ISSM	Janina Green(CTR)	AF/A4PA	janina.green.ctr@us.af.mil	(410) 382-8860

1. System Description

eTools Lite supplements or replaces Mobile Workstations (MWSs) with Commercial Mobile Devices (CMDs), specifically Apple iOS devices, which are typically used in conjunction with a lockable storage/sync/charging cart, hereafter referred to as 'cart', to store and view sensitive electronic Technical Order (eTO) and/or other sensitive/unclassified data up to FOUO, hereafter referred to as eTO/FOUO, information. The cart can store approximately thirty (30) iOS devices. The primary eTools Lite system components are iOS device(s), MacBook(s), external hard drive(s), and cart(s).

First, an authorized user's standard desktop configured PC (SDC) is used to download files needed for the eTools Lite implementation, in addition to eTO/FOUO information which is transferred to the iOS device. Needed implementation files include, but are not limited to, device software, mobile configuration profiles, lock screen image, MacBook policy banner text file, and other files detailed in the eTools Lite Authorized User Implementation Guide. iOS / MacBook device software updates, due to their large size, are typically downloaded directly from Apple servers. Users that cannot access the Apple servers from their SDC may download the updates directly to the MacBook using a trusted Wi-Fi connection. The specific links to the iOS device software files are posted on the AFTOFST SharePoint site and instructions to do this are in the eTools Lite Authorized User Implementation Guide.

Second, eTO/FOUO information is downloaded from its respective systems. For example, eTO documents are downloaded from ETIMS on the GCSS-AF network to the SDC. Because the MacBook is not allowed to be connected to the Air Force Network / GIG, an "air-gap" is needed to allow the MacBook access to the downloaded data. A DoD approved USB-based EHD is used to accomplish this "air-gap." Prior to using the EHD as an "air-gap," the device must first be scanned for malware (e.g. viruses) using the SDC's virus scanning application. If the SDC does not automatically scan the EHD when plugged in via USB, the authorized user must manually start and complete this malware/virus scan process by right clicking on the drive and selecting "Scan for threats…" from the drop down menu. The user will be prompted by the virus scanning application to either have it clean or delete the detected threats (i.e. malware, virus) if any are present. All detected malware must be reported IAW the User Rules of Behavior Agreement (AF Form 4433) and removed (i.e. cleaned or deleted) from the EHD prior to use. "Use" also implies if the EHD will only be connected to the MacBook to transfer/access files that are already on it and not just when data transfer from the SDC is involved.

Once the EHD has been verified as malware/virus free, the authorized user transfers all implementation files and needed eTO/FOUO information onto the EHD via USB connection. After transfer is complete, the EHD is unplugged from the SDC and plugged directly into one of the MacBook's USB ports. Files needed for the implementation of eTools Lite are transferred into the MacBook and used for device configuration IAW the eTools Lite Authorized User Implementation Guide. The iTunes application is used on the MacBook as a conduit to transfer the eTO/FOUO information from the EHD onto the iOS device. The Apple Configurator application on the MacBook is used to configure the iPads using a cart. Once iPads are configured and loaded with the needed eTO/FOUO information, the check-in/out process for iPads is handled by the Device Custodian. Device custodians are not authorized users and will not have access to the MacBook.

1.1. System Functions and Capabilities

1.1.1. User Safeguards

Authorized users will administer access based on defined user roles. The authorized users will maintain password configuration based on the procedures outlined in this document and applicable Security Technical Implementation Guide (STIG) guidelines. Authorized users, IAW with the eTools Lite Authorized User Implementation Guide, will use Apple Configurator to enforce restrictions on the iOS device in addition to the User Rules of Behavior Agreement (AF Form 4433) to achieve iOS configuration compliance per the SSP. The use of the eTools Lite Authorized User Implementation Guide will also enforce the required security hardening of the MacBook. Authorized users of the eTools Lite system are not required to possess a certification (A+, Network+, etc.) in order to administer eTools Lite devices since the Information System Security Manager (ISSM) dictates the security configuration. Adherence to the SSP and the Authorized User Implementation Guide will provide the necessary information to securely configure and maintain eTools Lite.

1.1.2. Applications for eTools Lite devices

The Configuration Control Board (CCB) must approve all changes to the eTools Lite hardware/software baselines IAW the CCB Process for eTools Lite. A list of approved applications can be found in the eTools Lite Hardware/Software Listing on the AFTOFST SharePoint.

1.1.3. Battery Life

Device Custodians should re-charge devices when the battery percentage goes below 30% to maximize device battery life. To avoid trickle charging, and ensuring maximum battery health, iOS devices should be unplugged once the devices reach full charge.

1.1.4. Screen Covers

All eTools Lite iOS devices must have adequate screen covers installed prior to initial use, as determined by the using organization. The purpose of the cover is to provide the screen minimum physical protection from common everyday use (e.g. scratches).

1.1.5. Protective Cases

All tablet devices should have a protective case prior to issue for use, creating a semi-rugged tablet configuration as approved by the MAJCOM, DRU, or FOA. The protective case should provide semi-rugged protection from weather elements and physical shock (e.g. rain, humidity, sand, and dust). The device should remain in the protective case at all times or, if not feasible, remain in the protective case from the time it is issued (i.e., checked out) by the Device Custodian until the time it is returned (i.e., checked in) to the Device Custodian. It is recommended that the protective case and the device be treated as a single eTools Lite component for hardware accountability purposes.

1.1.6. Deployment Support

Please refer to the deployment support policies that are specific to the eTO/FOUO information.

1.1.6.1. Deploying eTOs with iOS Devices

In instances where network connectivity is not assured, current technical data (i.e. eTOs) must be updated on all devices prior to departure and updated immediately upon return by authorized users IAW TO 00-5-1. Requirements could exist in a deployed mode requiring hard copies of eTOs.

For the majority of temporary duty (TDY) and short-term deployments (i.e. 60 days or less), IAW TO 00-5-1, iOS devices with current eTO updates are sufficient to support eTOs at locations other than home station. The authorized user will secure eTools Lite devices in a cart or other locked containers during transport. Standard physical controls will be used to secure the eTools Lite devices at the TDY/deployed location.

1.1.6.2. Deploying with eTools Lite Components

Bases that use eTools Lite typically have multiple carts, MacBooks and iOS devices. When a unit requires the full configuration at a TDY/deployed location, the authorized user will secure the eTools Lite components in a locked cart for transport to the TDY/deployed location. Standard physical controls will be used at the TDY/deployed location.

1.1.7. Connectivity

1.1.7.1. Wi-Fi

All Wi-Fi connections require FIPS 140-2 validated, password protected, WPA2 security. IAW with the CMD Wireless Policy V2R3 STIG, only cellular or site-managed Wi-Fi access point connected to the Internet only (Internet Gateway Only Connection) and home Wi-Fi network (user managed) WPA2 encrypted access points are authorized for eTools Lite components. WPA2 encryption (e.g. WPA2-PSK) must be used to safeguard Wi-Fi communications.

1.1.7.2. MiFi

MiFi is a personal hotspot device used to provide internet connectivity to devices that do not have cellular or WiFi connectivity. MiFi devices convert cellular signals to Wi-Fi. MiFi devices must be government purchased and authorized, and these devices must be FIPS 140-2 validated, password protected, and implement WPA2 security. These access points are connected to the Internet only (Internet Gateway Only Connection) and are to be used in the same way as a non-cellular Wi-Fi router in section 1.1.7.1 and IAW with AFI 17-130 (paragraph 4.7.2).

1.1.7.3. Cellular

Certain eTools Lite devices will have the capability to connect to commercial networks (.com) via cellular connection if the using organization’s use case requires it. Users should restrict Internet activity to sites that would normally be accessible using an Air Force Standard Desktop Configuration (SDC) computer.

1.1.7.4. Bluetooth Headsets

Bluetooth headsets have been approved for Unclassified use by BG Wooten (AFSPC/A6) in the memorandum *Bluetooth Peripherals Device*. As such, these devices may be used with the eTools Lite system for Unclassified communication.

1.1.7.5. BlueDriver On-Board Diagnostics II (OBDII) Connector

The BlueDriver OBDII connector is used primarily by the vehicle maintenance community and is a means of accessing manufacturer diagnostic codes produced by the vehicle using a special Bluetooth connector and a tablet. The information sent by the connector from the vehicle to the tablet does not contain any government data (all data is publically / commercially available), and is therefore approved for use with eTools Lite tablets. Some older vehicle models do not store the Vehicle Identification Number (VIN) on the vehicle's on-board computer. In this case, the VIN is entered manually and the BlueDriver app retrieves the vehicle information from a commercial database via the Internet. Once again, all of the data sent or received is publically / commercially available.

1.1.7.6. Mobile Device Management / Mobile Content Management

In certain cases, devices that are used with the eTools Lite system configuration also utilize a DoD-authorized MDM or MCM solution. The MDM and MCM solutions must be authorized by an Authorizing Official (AO) responsible for that system and are not part of the eTools Lite accreditation boundary. All established policies and procedures should be followed to ensure proper device security when using an MDM and/or MCM solution on eTools Lite devices. Devices that are managed via MDM rather than Apple Configurator must be configured and operated IAW the settings established in the eTools Lite SSP.

1.1.7.7. Internet Domain Whitelist Policy

For Cellular or Wi-Fi enabled deployments utilizing a DoD-authorized MDM (Mobile Device Management) solution with a domain whitelisting feature, internet domains should be authorized and whitelisted on an as-needed basis through the local unit's configuration change process. If the unit does not have an MDM or their MDM lacks a domain whitelisting feature, then users should restrict internet activity to sites that would normally be accessible using an Air Force Standard Desktop Configuration (SDC) computer.

1.1.7.8. Device-to-device Communications

Air Combat Command (ACC) has utilized appropriate contract vehicles to procure a cloud-based Microsoft Lync service hosted as part of Microsoft's Global Foundation Services (GFS) in a Government Community Cloud (GCC) facility that will be used with eTools Lite devices. The solution is FedRAMP certified and the communication via the Lync service is limited to Level 2 (publicly releasable) data to mitigate the risks associated with the use of this service. This service is an integral piece of the communications framework for parts delivery and maintenance operations on the flight line. Information regarding Microsoft's FedRAMP certification is available at the following URL: http://cloud.cio.gov/fedramp/microsoft.

Provided that the iCloud function remains disabled, users may also utilize the iMessage and FaceTime applications native to iOS for Level 2 (publicly-releasable) data / communications. Users should never discuss or share data above level 2 using either iMessage or FaceTime.

1.1.7.9. Approved DoD Multifactor Authentication

Thursby CAC readers, PKard Reader software, Yubikey, and other approved MFA solutions (IAW DoD Interim Digital Authentication Guidelines for Unclassified and Secret-level DoD Networks) are authorized for use with eTools Lite tablet devices.

MFA-enabled eTools Lite devices are only to be used to access approved DoD and Mission Partner enclaves and applications. These may be public-facing DoD applications (e.g., webmail, AF Portal, GuestNet), public-facing Mission Partner and AF-approved cloud-hosted applications, or protected, access-controlled enclaves accessed via the Internet (e.g., VPN-accessible .mil applications hosted in DoD data centers, Cloud One). The information system must be authorized to interface with eTools Lite.

1.1.8. eTools Lite Architecture

The eTools Lite architecture is dependent on the GCSS-AF architecture to download current eTO data from ETIMS. The eTools Lite architecture is separate and distinct from the ETIMS architecture; there are no networked or physical interfaces to Air Force Information System on the AF Global Information Grid (GIG). Specific policies for other FOUO information related to its transfer to the SDC must be followed. The highest level of information authorized to be stored on eTools Lite devices is Controlled Unclassified (For Official Use Only), Privacy Act, non-HIPAA, sensitive Scientific and Technical Information (e.g., eTOs).

1.1.9. System Resources

All eTools Lite components will be controlled on a local ADPE account (Device Code 0107) and in a tool accountability system or on an AF1297 IAW AFI 23-111. MAJCOMs will be able to data query on the ADPE for hardware baseline. AFSPC and DISA are the eTools Lite App approval authorities. The CCB authorizes all initial configuration components and subsequent changes to the software and hardware baselines for the devices (e.g. MacBook and iOS devices). A list of approved eTools Lite apps is maintained on the AFTOFST SharePoint.

1.1.10. FOUO Information Currency

Currency of FOUO information utilized by eTools Lite must comply with its respective update/currency policies and are executed by the authorized user. Section 1.1.10.1 provides an eTO currency example.

1.1.10.1. eTO Currency

Maintaining the currency of eTOs on the tablet devices is the responsibility of the authorized user. eTOs are updated on the devices weekly as directed by TO 00-5-1. The authorized user will download the Distribution Report into the eTools library and the maintainer will use it as a reference to verify the current version. A checklist should be used at each location to account for eTO currency. The checklist requires a detailed account of local process actions be given to the commanding authority prior to eTools Lite implementation.

The checklist will be signed by the commanding authority.

To comply with standard eTools update policy (TO 00-5-1), authorized users will transfer updated eTOs every seven (7) days (at a minimum) to ensure the most current versions are available to the user.

1.2. System Environment

To ensure proper functionality across diverse and challenging environments, Air National Guard Air Reserve Command Test Center (AATC) conducted operational utility evaluations on iOS devices to determine intrinsic safety, use in a Fuel Servicing Safety Zone (FSSZ) and Hazards of Electromagnetic Radiation to Ordnance (HERO) certification.

Based on their findings, iOS devices are considered intrinsically safe and can be used in a fuel servicing safety zone. Device specific test results can be found on the AFTOFST SharePoint. A copy of the report is also on file with AATC and the Enterprise Information Services SharePoint.

1.3. Description of Hardware and Software

1.3.1. Acquisition

The acquisition of hardware and software must comply with policy and guidance IAW AFMAN 17-1301 (Para 3.5) and the Air Force Information Technology and NetCentric Acquisition Guide. Hardware and software should be vetted and authorized through an officially recognized DoD validator such as:

- The Air Force Evaluated Products List
- DoD Application Vetting Environment
- The National Information Assurance Partnership
- DoDIN Approved Products List

1.3.2. iOS Devices

The authorized user will manage restricted settings for the iOS device via Apple Configurator or on-device IAW the most current Defense Information Systems Agency (DISA) iOS STIG.

Wi-Fi / Cellular capability must be disabled on the iOS device prior connection to the MacBook and must remain engaged as long as the iOS device is connected to the MacBook, either directly via USB port or via the charge / sync cart. This is accomplished by placing the iOS device in Airplane Mode prior to connection to the MacBook. This process prevents the possibility of creating a network bridge via multiple Wi-Fi or cellular network connections.

1.3.3. MacBooks

Step-by-step instructions on configuring the MacBook for the eTools Lite can be found in the eTools Lite Authorized User Implementation Guide on the AFTOFST SharePoint. The authorized account is used only when required for system configuration changes (e.g. system preferences). The authorized user manages user accounts via the authorized account. The non-authorized account is used for day-to-day operations (e.g. iTunes eTO/FOUO management). Separate MacBook user accounts and required authorized/non-authorized account types ensure least privilege rules are enforced. The MacBook is a non-AFNET connected stand-alone laptop.

User IDs will be removed and passwords disabled within 72 hours of notification that an authorized user no longer requires MacBook access. The guest account will be permanently disabled on all MacBooks. A DoD policy banner will be configured to display at the login window on the MacBook. File Vault 2 is enabled for FIPS 140-2 data-at-rest encryption on the MacBook.

1.3.4. External Hard Drive (EHD)

The DoD-approved EHD is connected to the MacBook. eTO/FOUO information is transferred from the EHD to iOS devices through the MacBook by using the iTunes / Apple Configurator application as a conduit. Other non-sensitive files that utilize the EHD for "air-gap," e.g. implementation files, can be transferred and stored on the MacBook. The EHD must be scanned for viruses upon being connected to the SDC or MacBook and cleaned of any viruses found before data is downloaded, prior to each data transfer from the SDC and/or to the MacBook. The eTO files can be retained on the EHD after they are successfully copied to the iOS devices by using the MacBook. External hard drives will be physically secured IAW AFI 23-111, AFMAN 17-1203, AFMAN 17-1301.

An additional DoD-approved EHD should be used to specifically backup Volume Purchase Program/Business-to-Business (VPP/B2B) licenses purchased for VPP apps by backing up the MacBook with Apple's native Time Machine backup software. This EHD must be separate from the EHD used for "air-gap" due to security requirements. The using organization will determine whether the MacBook is backed up, but the use of Time Machine for organizations that have purchased VPP/B2B software is strongly recommended to preserve license data. All backups will be protected by the MacBook FileVault encryption. If an EHD is used for backup, it must be secured in the cart or a Group Commander or equivalent approved locked drawer after each use. The backup will be FIPS 140-2 encrypted and implemented IAW the eTools Lite Authorized User Implementation Guide. Additionally, Time Machine backup disks should be stored in a lockable, AF-approved storage cabinet when not in use.

The acquisition, configuration, and usage of the EHD device should be in compliance with the following:

1. The acquisition of the device should adhere to AFMAN 17-1301 (Para 3.5) and the Air Force Information Technology and NetCentric Acquisition Guide.
2. The user of the device should have a signed DoD "Removable Storage Media Acceptable Use User Agreement" on file (available on the AFTOFST SharePoint)
3. The EHD device should only be used to air-gap FOUO electronic technical order (eTO) data exported from ETIMS for use on eTools Lite devices
4. The configuration for encryption of the device adheres policy in AFMAN 17-1301 (paragraphs 4.7 and 4.12) and the following guidance in DISA's "Removable Storage and External Connections Security Technical Implementation Guide (v1r7)":
    a. STO-DRV-010: Access to mobile and removable storage devices such as USB thumb drives and external hard disk drives will be protected by password, PIN, or passphrase.

b. STO-DRV-020: Sensitive but unclassified data must be encrypted using FIPS 140-2 validated modules when stored on a USB flash drive and external hard disk drive.
c. STO-DRV-025: Configure the cryptographic module on a USB thumb drive or external hard drive using a NIST-approved encryption algorithm to encrypt sensitive or restricted data-at-rest.

5. The removable storage media device should be immediately scanned for viruses upon connecting to an Air Force SDC computer or the eTools Lite administrator MacBook
6. The physical security and asset management should adhere to policy outlined in AFI 23-111, AFMAN 17-1203, AFMAN 17-1301
7. The media sanitization of the external hard drive contents adheres to DoDI 8500.01 (section 9.b.9) and to NIST Special Publication 800-88r1 "Guidelines for Media Sanitization"

1.3.5. Standard Desktop Configuration (SDC) Computers

Organizations that use tablet devices and do not have access to a MacBook can typically use an SDC computer to transfer data to the tablets. Please contact your local communications squadron to determine what additional steps are required (e.g. white listing / serial number registration) prior to connecting the tablet devices to an SDC.

NOTE: Do not use personal computers / non-SDC computers (other than the eTools Lite MacBook) to transfer sensitive government data.

1.3.6. Approved Software / Hardware

For a complete listing of hardware and software approved for use with the eTools Lite system configuration, please refer to the eTools Lite Hardware / Software Listing on the AFTOFST SharePoint.

1.4. Supported Mission

eTools Lite devices are used in diverse and demanding operational environments such as maintenance hangars, tool rooms, and out on the flight line in support of multiple installation and mission support activities. The primary purpose of the system is for use in the performance of logistics, installations, and mission support duties which require the viewing of electronic technical orders.

1.5. Data Types / Protection Methods

The eTools Lite system stores / processes publically-releasable (level 2) data and sensitive / unclassified data up to FOUO / CUI (level 4). The eTools Lite system does not store personally identifiable information (PII) or classified data.

Common Types of Sensitive Information Processed by eTools Lite (level 4):

- electronic Technical Order (eTO) data
- How-To Videos (H2Vs) for aircraft repair

Common Types of NON-Sensitive Information Processed by eTools Lite (level 2):

- MS Lync communication
- Vehicle maintenance / diagnostic data
- Public web sites

While it is important to be cognizant of the sensitivity level of the data being stored / viewed / processed by the device at any given time, all eTools Lite devices are configured to keep sensitive data secure. This ensures that the end user is not responsible for managing, or permitted to alter, security measures on the devices. All devices are secure by default.

For technical instructions on data protection, refer to sections within the System Security Plan for guidance on configuring components to protect data-at-rest, data-in-transit, network security, physical security, and media sanitization.

1.6. System Availability

eTO data availability is dependent upon the Enhanced Technical Information Management System (ETIMS) as the primary data source for eTO data used with the eTools Lite system. Hardware components of the system are mainly comprised of easily-replaced end-point devices that can be substituted should a failure occur. For a complete overview of the system Continuity of Operations (COOP) process, please reference the Authorized User Implementation Guide which can be found in the document library section of the AFTOFST SharePoint.

1.7. Backup and Recovery

For backup and recovery, the Authorized Users Guide (found in the document library section of the AFTOFST SharePoint) contains instructions on:

- How to use the Apple Configurator on the admin MacBook to create a master image of an iPad baseline and restore it to multiple iPads that needs to be refreshed or restored.
- How to use the MacBook’s Time Machine native backup application for to backup VPP (Volume Purchase Program) licenses that Apple Configurator has used to install VPP apps onto the iPad from a single MacBook. The backup will help reduce the risk that licenses are lost in certain cases (e.g., MacBook storage failure).
- How to backup and restore electronic technical orders (eTOs).

1.8. Supporting Documentation

This System Security Plan (SSP) will be reviewed and updated at least annually or more frequently as required to ensure that the policies support system operations. The SSP and other supplementatl eTools Lite documentation will be uploaded to the AFTOFST SharePoint and be placed within the Document Library in the section named “AFTOFST Field User Guides”.

The AFOFST contact information is:

- Email: af.etimstofst@us.af.mil

- URL: https://cs2.eis.af.mil/sites/12982/default.aspx
- Phone: DSN: 872-9300 or COM: 850-882-9300
- Office Hours: 0800-1600 hrs CT, Monday-Friday

Additionally, when changes to the Sytem Security Plan or supplemntal eTools Lite documention are released, the MAJCOM point of contacts require notifiation (available on the AFTOFST SharePoint).

2. System Topology

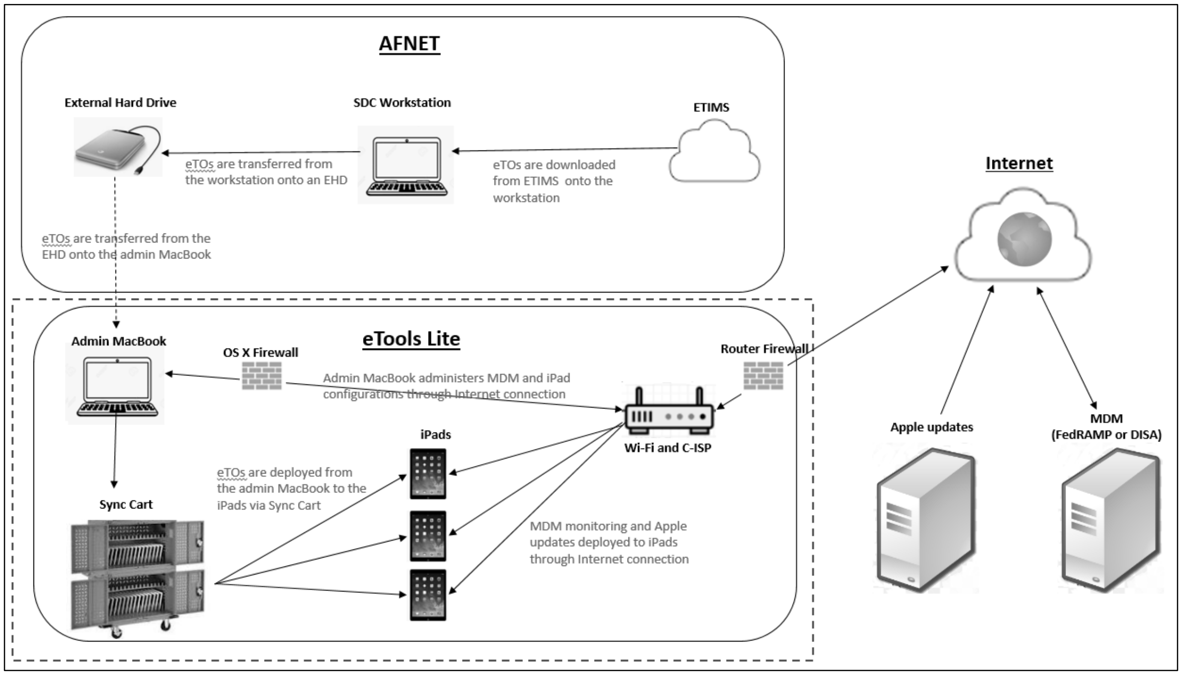
AFNET
External Hard Drive
SDC Workstation
ETIMS
eTOs are transferred from the workstation onto an EHD
eTOs are downloaded from ETIMS onto the workstation
eTOs are transferred from the EHD onto the admin MacBook
Internet
eTools Lite
Admin MacBook
OS X Firewall
Router Firewall
Admin MacBook administers MDM and iPad configurations through Internet connection
iPads
Wi-Fi and C-ISP
Apple updates
MDM
(FedRAMP or DISA)
Sync Cart
eTOs are deployed from the admin MacBook to the iPads via Sync Cart
MDM monitoring and Apple updates deployed to iPads through Internet connection

Figure 1: eTools Lite Architecture

2.1. System Interfaces

The eTools Lite system has 12 interfaces:

1. External HD to MacBook
2. MacBook to Tablet Device(s)
3. Wi-Fi
4. Cellular (optional)
5. Tablet device to Mobile Device Management Server / Mobile Application Store (MDM/MAS) (optional)
6. Tablet device to Mobile Content Management (MCM) Server (optional)
7. Tablet device to Microsoft Lync Server (optional)
8. Tablet device to Bluetooth Headset (optional)
9. Tablet device to CAC Reader (optional)
10. MacBook to Time Machine backup disk (optional)
11. Tablet device to BlueDriver OBDII Connector (optional)

3. Users, Locations, and End Point Devices

3.1.1. System Access Rules & Policy

Users of the eTools Lite system will use eTO/FOUO information on tablet devices in the daily performance of logistics, installations and mission support activities. The required training and agreements needed for the use of eTools Lite itself is outlined in section 3.1.5. Any additional requirements, training, and agreements needed as a result of the eTO/FOUO information utilized with eTools Lite devices is to be completed IAW their applicable AFI(s), rules, and regulations. Technical Order Distribution Officer (TODO)/Quality Assurance (QA)/Supervisor or Role Equivalent will establish physical asset control, conduct user training, assign user roles and monitor daily use. Major Command (MAJCOM), Direct Reporting Unit (DRU), Field Operating Agency (FOA) policy and information analysis will be used to ensure definition of duties; need-to-know access and data confidentiality are maintained. MAJCOM POC's will be listed on the AFTOFST SharePoint.

3.1.2. Account Management

The Group Commander or equivalent will designate the authorized users through an appointment letter that will be retained at the unit in the individual's file agreement folder. The Group Commander or equivalent will ensure the individuals have the appropriate clearance; meets the training requirements; and have a need-to-know based on individuals' duties and responsibilities IAW AFI 21-101.

Authorized users will establish group accounts for non-authorized users and ensure all required agreements for non-authorized users are completed and stored at the unit in the individual's file agreement folder.

Group Commander or equivalent will periodically review the authorized account holders and retains the authority to terminate authorized and non-authorized account privileges based on the severity of violations to the User Rules of Behavior Agreement (AF Form 4433) and Authorized User Agreement (available on the AFTOFST SharePoint).

3.1.3. User Permission Matrix

The following table establishes the class and system permissions relationship for users and eTO/FOUO data.

Table 3: User Permission Matrix

	USER ROLES	CONFIGURE eTools Lite Devices	ADD/DELETE USER ACCT	READ	DELETE	UPDATE eTOs
	System Engineer	X	X			
Authorized User	TODO/QA/Supervisor or Role Equivalent	X	X	X	X	X
	Assistant TODO/QA/Supervisor or Role Equivalent	X	X	X	X	X
	Contractor TODO[1]	X	X	X	X	X
	Device Custodian			X		
	Standard User			X		
	Foreign Nationals[2]	NONE	NONE	X	NONE	NONE

Authorized users are defined as the TODO/QA/Supervisor or Role Equivalent, the Assistant TODO/QA/Supervisor or Role Equivalent, Contractors, and TODOs performing major duties including, but not limited to supervising accountability and storage procedures for the eTools Lite devices; managing device configuration; and provisioning of tablet devices with all applicable configuration settings and data libraries. TODO/QA/Supervisor, Assistant TODO/QA/Supervisor, and their Role Equivalent are defined as any individuals authorized by the Group Commander or equivalent to perform the duties and responsibilities of the TODO/QA/Supervisor or Assistant TODO/QA/Supervisor, respectively. Authorized users will sign an Authorized User Agreement (available on the AFTOFST SharePoint) that will be maintained at the unit in the individual's file agreement folder. Group Commander or equivalent

[1] Contractors who require similar eTO access to TODO/QA/Supervisor or Role Equivalent and Assistant TODO/QA/Supervisor or Role Equivalent will need to fulfill all "Contractor TODO" requirements IAW TO 00-5-1. Contractors who require access to other FOUO information must comply with the FOUO's respective policies. All users, including contractors, must also fulfill and meet all expectations set out within section 3.1.5.

[2] The Group Commander or equivalent will ensure that Foreign Nationals have the appropriate clearance, meet the training requirements, and have a need-to-know based on the foreign national authorized user's duties and responsibilities IAW AFI 21-101. See section 3.1.4 for additional details on Foreign National use.

should authorize authorized users the rights and privileges. TODO/QA/Supervisor or Role Equivalent, Assistant TODO/QA/Supervisor or Role Equivalent, Contractors, and TODOs will hereafter be referred to as authorized users. Device Custodians are not authorized users and will not have access to the MacBook. Additionally, the transfer of eTO/FOUO information from the SDC computer with an EHD to iOS devices via the MacBook does not require an authorized user account.

3.1.4. Foreign Nationals

Two scenarios exist where foreign government individuals will interact with the eTools Lite System:

a. The first scenario involves foreign national logistics personnel working on AF bases overseas. In this case, a foreign national will be granted read access to technical orders and other FOUO information by the eTools Lite authorized user for the purpose of completing a maintenance or logistics activity. The authorization to view technical data is determined by the Authorized User in accordance with TO 00-5-1 Chapter 7 and DoDI 5200.48 (Section 3.4).
b. The second scenario involves the use of the eTools Lite system configuration by the Royal Netherlands AF (RNLAF). The system will be used to view RNLAF technical data on RNLAF-owned devices only. No U.S. DoD information will be viewed, stored or processed by this system, and no U.S. devices will be used. The Foreign Affairs Specialist in SAF/IAPD, Foreign Disclosure and Technology Transfer Division Policy Directorate has reviewed the eTools Lite SSP and cleared the document for release to the RNLAF for review and implementation of the eTools Lite system configuration.

3.1.5. Access to eTools Lite

Access to eTools Lite is established based on the following criteria:

1. Users must have a valid need-to-know and the appropriate security clearance for the data on the devices
2. All users must complete the DISA Smartphone and Tablet Training.
3. All users must sign User Rules of Behavior Agreement (AF Form 4433)
4. Authorized users will maintain a signed User Rules of Behavior Agreement (AF Form 4433) for each eTools Lite user
5. Authorized users, in addition to the User Rules of Behavior Agreement (AF Form 4433), will also need to complete an Authorized User Agreement (available on the AFTOFST SharePoint) and be maintained IAW the account management process outlined in this document
6. Device custodian will use tool accountability system or use AF1297 IAW AFI 23-111 for device check-in/out
7. Users will be deleted from tool/device accountability system during out processing or destroy the AF1297 IAW AFI 23-111
8. Authorized users will maintain device security configurations in accordance with this SSP

3.1.6. User Rules of Behavior

Authorized behavior of system users, includes privileges assigned to user categories outlined in the matrix in section 3.1.3. Subject to the User Rules of Behavior Agreement (AF Form 4433) users are accessing a U.S Government (USG) system that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), the individual consents to policies associated with official usage. Failure to adhere to the policies will result in non-judicial or judicial punishment IAW AFI 10-712, AFI 23-111, and AFI 17-130. The User Rules of Behavior Agreement (AF Form 4433) will be administered locally by the using organization and remain on file with the unit in the user file agreement folder for each individual, to facilitate administrative actions relative to violation of established User Rules of Behavior Agreement (AF Form 4433). The use of digital signatures is authorized to indicate user acknowledgement of the User Rules of Behavior Agreement (AF Form 4433). All authorized users, in addition to the User Rules of Behavior Agreement (AF Form 4433), will also need to read and sign the Authorized User Agreement (available on the AFTOFST SharePoint).

3.1.6.1. Additional User Agreement Guidelines

- The eTools Lite components (including Sync/Charging cart, external hard drive, MacBook, and iOS devices) will only be used for the storing, viewing, and annotating of sensitive data, and other data up to FOUO content when properly configured.
- All MacBooks and tablet devices must be configured, by trained authorized users only, in accordance with the eTools Lite Authorized User Implementation Guide that is posted on the AFTOFST SharePoint. Non-authorized users are not allowed to change settings on any eTools Lite components.
- All eTools Lite components will be turned off and secured when unattended. Any damage to components will be immediately communicated to the commanding Authorized User, in addition to the requirements set forth below in the User Rules of Behavior Agreement (AF Form 4433).
- eTools Lite components will never be used for (1) an entertainment device for viewing or playing film, music, games, or taking personal photographs; (2) unauthorized connection to the SDC or any DoD / Air Force network (3) storing any unauthorized personal information or using any of the restricted/do-not-use Apps, as defined in the eTools Lite Authorized User Implementation Guide; (4) installing or using any Applications not listed as approved on the SharePoint except for authorized testing.

In addition to the guidelines above, ensure you are following the security configuration and usage provisions for your specific device outlined in section 3.1.11.

3.1.7. Failure to follow User Rules of Behavior or Authorized User Agreement

Inappropriate use will be reported to the Group Commander or equivalent for disciplinary action IAW the User Rules of Behavior Agreement (AF Form 4433) and the Authorized User Agreement. Unit violations will be tracked by the Group Commander or equivalent and briefed to appropriate MAJCOM, DRU, or FOA leadership.

3.1.8. Physical Security

Information displayed by eTools Lite is considered sensitive, i.e. Controlled Unclassified Information (CUI), and is marked or labeled according to DoDI 5200.48 (Section 3.4) and DoDI 5230.24. Markings and labels clearly reflect the sensitivity level, if applicable, and any special dissemination, handling, or distribution instructions. Physical security of eTools Lite devices in compliance with AFI 23-111 (section 2.7.2) and DoD 5200.08-R requires that Group Commanders or equivalent will provide adequate security, storage facilities, and accountability procedures to protect and secure eTools Lite components. Potential risks to the AF network are mitigated by requiring individuals to sign out a device, and holding each individual accountable for the device until it is returned to an access control point (e.g., Maintenance Support Section). To ensure standardization among maintenance units, commanders and key leaders are responsible for executing an effective program IAW AFI 21-101. Authorized user/Consolidated Tool Kit (CTK) Custodian will complete an end of day activity security checklist (i.e. SF 701) to include eTools Lite components (cart, tablet devices, MacBook, EHD) returned/secured unless properly accounted for and signed out on an AF1297 IAW AFI 23-111 or through a Tool accountability System (TAS) as outlined per AFI 21-101.

The following is an example of what is meant by “adequate storage facilities”: A tool room/tool issue center must be capable of being locked and afford protective measures such as monitoring, 24-hour coverage, or controlled key access IAW AFI 21-101. When all CTKs/TKs are not capable of being secured in the tool room/tool issue center, the section Non-Commissioned-Officer-In-Charge (NCOIC)/Tool issue center/authorized user will design a process to prevent the unauthorized use or access to tools and equipment IAW AFI 21-101. Tool kit locks will be used to provide a physical barrier to prevent the unauthorized removal of tools. Locks are not required on tools and equipment that are stored within secured tool rooms or work centers.

3.1.8.1. Hardware Accountability

All eTools Lite components (e.g., tablet devices, MacBook, EHD, and cart) will be treated as government property in possession of the Air Force IAW AFI 23-111. As such, the Group Commander or equivalent is required to provide adequate security and storage facilities and accountability procedures to protect and secure government property. Such property (e.g., eTools Lite components) will be controlled on a local ADPE account (Device Code 0107). It is also highly recommended that the devices be tracked in a tool accountability system or by AF1297 IAW AFI 23-111 when used as part of a maintenance program.

For example, the process for tools requiring physical security is established in AFI 21-101. These devices will be controlled using standard tool/equipment accountability procedures resident in the maintenance environment. The procedures provide detailed, shift-by-shift control of assets ensuring an extremely high level of accountability. In accordance with AFI 21-101, all e-Tools purchased and used for the purpose of viewing digital technical data and/or for maintenance documentation must be accounted for as automated data processing equipment (ADPE) IAW AFI 33-112 and other 33 series AFIs and tracked in TC Max or other approved tool accountability system. The equipment will be controlled on a local ADPE account (Device Code 0107) and in a tool accountability system or by AF1297 IAW AFI 23-111.

All devices containing sensitive / FOUO information will be kept within government control at all times. If a device is used for training purposes or other use cases that do not require the storage of sensitive / FOUO data, the device may be transported outside government control if permitted by the using organization.

3.1.9. Network Security

iOS devices are permitted to connect to the internet using a field location's authorized DoD-managed Wi-Fi hotspot, approved commercial ISP Wi-Fi hotspot, or using an authorized cellular connection. Wi-Fi connections must implement FIPS 140-2 WPA2. Cellular connections must implement FIPS 140-2 encryption (e.g., IPsec, TLS) from the mobile end point to an authorized encrypted tunnel termination point.

Internet connectivity is only to be used to access approved DoD and Mission Partner enclaves and applications. These may be public-facing DoD applications (e.g., webmail, AF Portal, GuestNet), public-facing Mission Partner and AF-approved cloud-hosted applications, or protected, access-controlled enclaves accessed via the Internet (e.g., VPN-accessible .mil applications hosted in DoD data centers, Cloud One). The information system must be authorized to interface with eTools Lite.

Encryption is used on the iOS devices to protect stored sensitive data (i.e. data-at-rest). iOS devices must be securely configured in accordance with relevant DISA Security Technical Implementation Guides (STIGs) and Security Requirements Guide (SRG) and must implement the eTools Lite configuration profile.

MacOS devices will need FIPS 140-2 WPA2 wireless encrypted commercial network connectivity to Apple servers to complete iOS device provisioning procedures. Encryption is used on the eTools Lite MacBooks to protect the stored sensitive data (i.e. data-at-rest). A DoD approved EHD is utilized to "air gap" iOS device software, eTO/FOUO information, mobile configuration profiles, and other needed configuration files from the network device to the tablet devices, utilizing the MacBook as a conduit for the transfer IAW the eTools Lite Authorized User Implementation Guide. MacOS devices must be securely configured in accordance with relevant DISA Security Technical Implementation Guides (STIGs) and Security Requirements Guide (SRG) and must implement the eTools Lite configuration profile.

3.1.10. System Configuration Management

Software updates for the MacBooks and iOS devices are installed as prescribed by USCYBERCOM's Information Assurance Vulnerability Management (IAVM) notices, and must be installed to ensure continued compliance with DoD policy. The eTools Lite Information System Security Manager (ISSM) approves and manages the priorities and timing for enhancements and upgrades not covered by IAVMs. A system patch log tracks OS X and iOS software security patches and updates that have undergone functional and regression testing by the system engineer, and ultimately approved by the eTools Lite ISSM.

eTools Lite version number is incremented to account for any changes prescribed by IAVMs or other approved patches/updates. eTools Lite authorized users should ensure that the most current software version prescribed by the eTools Lite Patch Log is installed within ninety (90) days of the eTools Lite version release unless upgrades will result in a significant negative impact to the using organization. In such a case, the organization will work with the eTools Lite Program Office to mitigate the security risks associated with failure to upgrade and create an implementation timeline/POA&M for migrating to the new version.

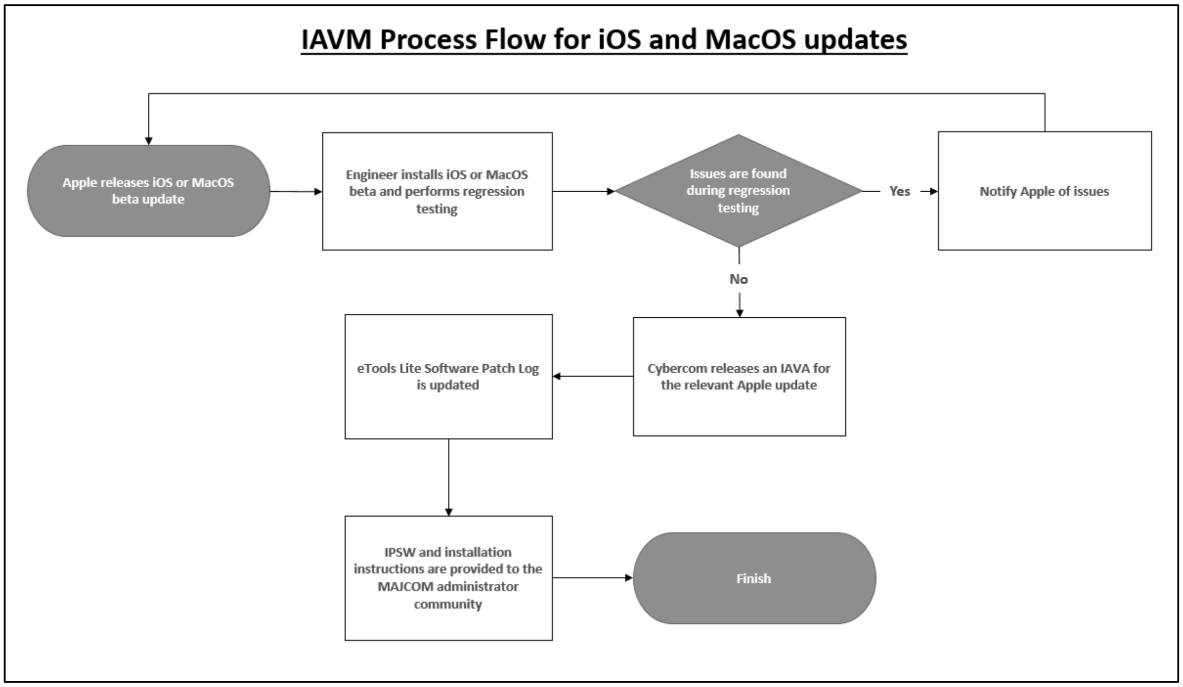
IAVM Process Flow for iOS and MacOS updates
Apple releases iOS or MacOS beta update
Engineer installs iOS or MacOS beta and performs regression testing
Issues are found during regression testing
Yes
Notify Apple of issues
No
Cybercom releases an IAVA for the relevant Apple update
eTools Lite Software Patch Log is updated
IPSW and installation instructions are provided to the MAJCOM administrator community
Finish

Figure 2: Process Flow for Vulnerability Alerts and Security Patches

3.1.11. Device Configuration Policy

All eTools Lite devices are configured IAW applicable DISA STIG requirements. The eTools Lite Authorized User Implementation Guide documents the required configuration and implementation procedures to ensure proper functionality and security compliance and can be found on the AFTOFST SharePoint. Additional information regarding the specific STIG checks performed can be found in the eTools Lite Security Assessment Plan (SAP), and within the associated test plans.

These listed settings are considered "restricted settings." Only authorized users are permitted to manage these "restricted settings."

3.1.11.1. iOS Devices

iOS devices are configured via device profiles developed by the eTools Lite project office. The applicable STIG configuration settings for eTools Lite iOS devices are available on the AFTOFST SharePoint.

Field units whose inventory include older generation iPads that Apple Servers are no longer signing or supporting the device's iOS software may continue to operate these devices if the following security mitigations are implemented on the unsupported device by the units eTO manager (TODO):

1. Using an approved "Restricted Profile" to hide all native default apps from field users.
2. Restricting the ability to connect to the internet when not in the possession of the eTO manager (TODO). This is accomplished by placing the iPad in "Airplane" mode.

Otherwise the unit or MAJCOM Reps must purchase new replacement iOS devices (iPad) which are supported by Apple updates.

3.1.11.2. Mac OS Devices

Mac OS devices are configured via device profiles developed by the eTools Lite project office. The applicable STIG configuration settings for eTools Lite Mac OS devices are available on the AFTOFST SharePoint.

Due to the disconnected configuration, there is not a centralized network audit capability to monitor user access for eTools Lite MacBooks, as they are not authorized to be connected to AFNET or any government network. The MacBook generates audit records directly on the machine that are in compliance with the Apple Mac OS Security Technical Implementation Guide (STIG). Upon ISSM request, MacBook audit records will be exported and sent to MAJCOM POCs and the ISSM for periodic review. Instructions on generating the record can be found in the eTools Lite Authorized User Implementation Guide.

3.1.12. iCloud / Online File Sharing

The eTools Lite configuration does not permit the use of iCloud or other methods of online file storage or sharing. Users must not enable iCloud or any other feature of either iOS or individual apps that would enable this capability. Use of the Abode Reader Mobile Link functionality for online file storage is expressly prohibited.

3.1.13. Remote Access

The eTools Lite configuration does not permit remote access to any of its components (which includes iPads and MacBooks). The eTools Lite iOS and MacOS configuration profiles are configured in accordance to their respective DISA STIGs, and both the iOS and MacOS STIGs require all settings for remote access to be disabled.

4. Authorized User Training Requirements

The ISSM meets training and certification requirements of DoD 8570.01-M, Information Assurance Workforce Improvement Program, for ISSM Level I.

In addition to the DISA Smartphone and Tablet Training, Authorized users must also complete the Privileged User Cybersecurity Responsibilities Training and must meet all DoD level requirements for end user awareness training IAW DoD 8570.01-M. All authorized users must read and be familiar with the eTools Lite Authorized User Implementation Guide, which can be downloaded from the AFTOFST SharePoint. Training should be conducted by experienced iOS device authorized users.

Authorized users must conduct local training for other authorized users. All users must be in compliance with the annual AF DoD IA training requirement. All end users will report suspicious activity associated with information systems and mobile devices to the authorized user and/or their Group Commander or equivalent. Vulnerabilities will be identified and reported using guidelines prescribed in the User Rules of Behavior Agreement (AF Form 4433).

The Group Commander or equivalent completes a post-training checklist to ensure User Rules of Behavior Agreement (AF Form 4433) and Authorized User Agreement requirements are defined/implemented; once all actions are complete, the unit will be declared a Full Operational Capability (FOC).

5. Media Sanitization and Physical Breakage/Damage

If an eTools Lite component that has ever stored eTO/FOUO information physically breaks, then the NIST SP 800-88 device sanitization and verification procedures (as further described in section 5.1) should be adhered to before sending it back to the manufacturer for repair or a technician is brought to repair the device.

Devices that have sustained physical damage and have been repaired are no longer compliant with HERO standards, and should not be used in an area where HERO certification is required. The MAJCOM will track/review capability and cost factors. Follow local MAJCOM policy to procure new components if needed.

5.1. Media Sanitization

Air Force policy memorandum AFMAN 17-1301 (section 6.2 Sanitization) adheres to NIST SP 800-88 (Guidelines for Media Sanitization).

For proper sanitization of Apple iOS devices, in NIST SP 800-88 figure 4-1 (Sanitization and Disposition Decision Flow) refer to table A-3 (Mobile Device Sanitization). In table A-3, the instructions for Clear/Purge of Apple iOS devices should be adhered to.

For sanitization of other types of media, also refer to NIST SP 800-88 for guidelines.

5.2. Repairs

If restoring from a backup does not repair a damaged component, then perform media sanitization prior to sending to the vendor for device repair or disposing of a component. Please refer to your MAJCOM POC for questions related to the reformatting of the EHD and the MacBook. When reformatting the EHD, ensure that a windows/mac compatible format (e.g., ExFAT) is used.

5.3. Re-Provisioning

In the event an eTools Lite device needs to be re-provisioned to another government facility/team, a factory reset is performed which deletes the device encryption keys, making all stored data unreadable. Instructions to do this are documented within the eTools Lite Authorized User Implementation Guide, which is available on the AFTOFST SharePoint.

6. Policy & Procedures Overview for eTools Lite Users

6.1. MAJCOM

1. Provide overall strategy and plan including budget, plan, and fielding of eTools Lite devices.
2. Manage the site survey and activation.
3. Serve as site activation decision authority.
4. Plan and coordinate with eTO/FOUO managers and authorized users to implement disconnected operations within the overall ETIMS environment.
5. Provide help desk guidance.
6. Procure new eTools Lite components as needed IAW local MAJCOM policy.
7. Procure Volume Purchase Program (VPP) / B2B apps and distribute to authorized users as needed.
8. Destroy eTools Lite components as needed IAW AFMAN 17-1301.
9. Provide adequate procedures for the secure storage of MacBook audit records.

6.2. Group Commander or Equivalent

1. Identify the authorized users and, if applicable, assistant authorized users.
2. Ensure that at least one authorized user is assigned to the MacBook at all times.
3. Designate authorized users through an appointment letter.
4. Certify all authorized users have the eTO/FOUO specific appropriate clearance and training requirements, and have completed the User Rules of Behavior Agreement (AF Form 4433) and Authorized User Agreement.
5. Complete a post-training checklist to ensure User Rules of Behavior Agreement (AF Form 4433) and Authorized User Agreement requirements are defined/implemented.
6. Certify all training and the User Rules of Behavior Agreement (AF Form 4433) has been completed and sustained for all users.
7. Ensure authorized users are trained on set-up procedures.
8. Maintain strict tool and equipment control/use standards.
9. Enforce disciplinary actions as required.
10. Provide adequate security, storage facilities, and accountability procedures to protect and secure eTools Lite components IAW AFI 23-111.
11. Provide overall management of the program.

6.3. Authorized User

1. Maintain signed User Rules of Behavior Agreement (AF Form 4433) for Device Custodians and Users and copies of local training requirements/checklists used for eTools Lite. Maintain these documents until at least six months after the user no longer requires access.
2. Determine which eTO/FOUO information is needed.
3. Ensure required eTO/FOUO currency.
4. Ensure latest CCB approved implementation files are used. This includes attaining the latest required implementation files on the EHD (e.g. iOS Device Software, DISA STIG iOS mobile configuration profile, eTools Lite mobile configuration

profile, etc.) from the AFTOFST SharePoint as instructed in the eTools Lite Authorized User Implementation Guide.

5. Generate MacBook audit records upon request.
6. Conduct random checks to ensure approved eTools Lite configuration is maintained IAW instructions provided in the eTools Lite Authorized User Implementation Guide.
7. If applicable, determine which eTO/FOUO information is made available to approved foreign nationals.

6.3.1. Additional Authorized Users Program Support

1. Identify, train and manage assistant authorized users.
2. Change PIN on all devices per section 3.1.11.
3. Refine tablet device and cabinet quantities for each iOS device storage location (e.g., facilities, buildings, hangers, etc.) within allocated funding levels.
4. Identify site preparation requirements to support tablet devices and cabinets (e.g., power, Wi-Fi connectivity, support computers, cooling, etc.)
5. Inventory and inspect tablet device.
6. Load/Gain equipment on accountable records.
7. Disperse tablet devices to pre-designated storage locations.
8. Backup MacBook if required by using organization.
9. Adhere to the eTools Lite Authorized User Implementation Guide.

6.3.2. Assistant Authorized Users

- Duties as assigned by the Authorized User.

6.4. Device Custodian

1. Specifically note if there is any problem recharging the battery once the battery charge level falls to or below 30% (i.e., the percentage at which the battery should normally be recharged).
2. Recharge tablet devices when the battery percentage goes below 30% to maintain battery health.
3. Provide authorized users information on any problems encountered (note any damage, complete damage reports, etc.).
4. Use tool accountability system or AF1297 for equipment accountability.
5. Manage protective cases and screen protectors.
6. Ensure that eTools Lite devices are only distributed to personnel with a valid need-to-know, and that these individuals have the appropriate security clearances for the device and the information stored on the device (this includes foreign nationals, if applicable for the using organization).

6.5. Standard User

1. Check out device from the tool accountability system or with AF1297.
2. Power on device.
3. Note battery setting.
4. Ensure safe and compliant usage.

5. Shut down tablet device when not in use.
6. Return device to checkout location.
7. Report any damage/issues to Device Custodian.

7. Security Funding Strategy

The Directorate of Systems Integration will fund two FTEs responsible for the sustainment of the eTools Lite Authority To Operate (ATO) across the Fiscal Year Development Plan (FYDP).

8. Audit Review, Analysis, and Reporting

The A4PA Mobile Technology Branch ISSM will conduct bi-annual audit assessments to ensure the field complies with the security policy listed in the eTools Lite System Security Plan. The ISSM will coordinate audit assessments with eTools Lite MAJCOM implementations and evaluate the compliance of logical and physical security with the eTools Lite System Security Plan. The template for the compliance assessment can be found on the AFTOFST SharePoint.

If unauthorized activity is discovered during an audit, the appropriate contacts for each MAJCOM can be found on the AFTOFST SharePoint.

9. Technical Support

There are multiple levels of support depending on whether an issue is isolated to one specific device with malfunctioning hardware or the issue is a wider spread software or operating system issue. The levels of support include:

1. **Custodian** – provides support to Standard Users.
2. **TOFST (AF TO Field Support Team)** – Device errors are not resolvable by the local MAJCOM Custodian, they will be escalated to the Technical Order Field Support Team (TOFST) for tier 1 & 2 helpdesk support.
3. **A4PA/ELMS Technician** - Unresolved issues will be escalated from the TOFST to the A4PA/ELMS Technician for tier 3 support.

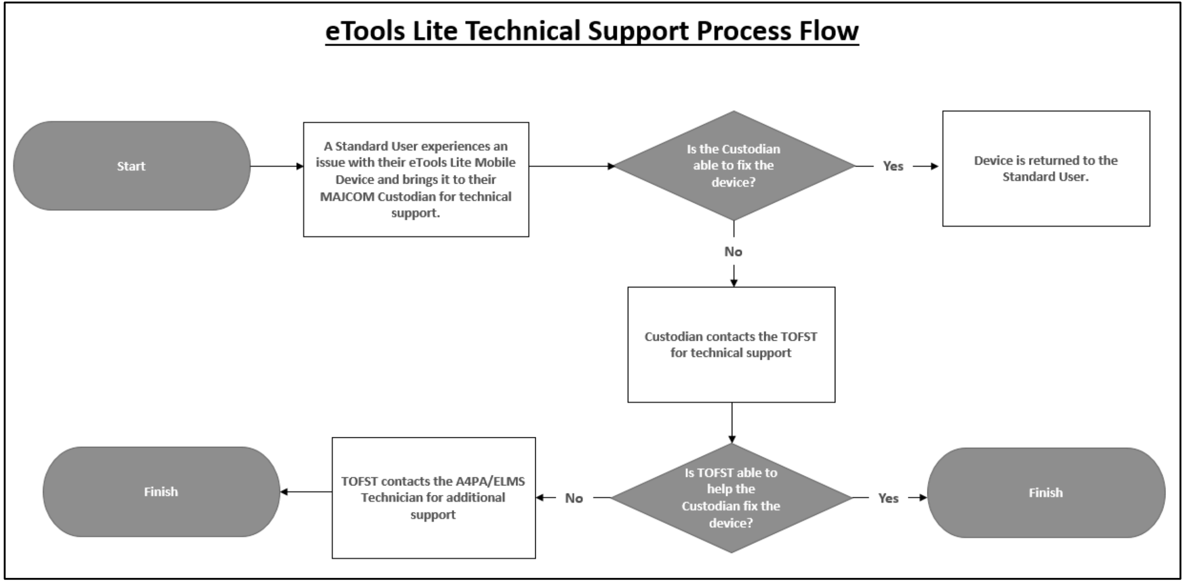
eTools Lite Technical Support Process Flow
Start
A Standard User experiences an issue with their eTools Lite Mobile Device and brings it to their MAJCOM Custodian for technical support.
Is the Custodian able to fix the device?
Yes
Device is returned to the Standard User.
No
Custodian contacts the TOFST for technical support
Is TOFST able to help the Custodian fix the device?
Yes
Finish
No
TOFST contacts the A4PA/ELMS Technician for additional support
Finish

Figure 3: Process Flow for Technical Support

10. Incident Response

The Incident Response for eTools Lite depends on the type of incident, assets, and personnel involved in the incident. The types of eTools Lite IT assets include:

1. iPads
2. MacBooks
3. External Hard-Drives
4. Wireless Routers
5. Sync Carts
6. Electronic Technical Orders and sensitive/unclassified data up to FOUO

If any assets are damaged, missing, stolen, hacked, or there is data spillage, the incident should be immediately reported to the Wing ISSM and Custodian so that the severity and remediation can be properly assessed. If the incident severity is determined to be HIGH then MAJCOM leadership and the A4PA Program Level ISSM should be notified. HIGH severity incidents will adhere to guidance in NIST SP 800-61 Rev. 2 “Computer Security Incident Handling Guide” for remediation and post-incident analysis.

Additionally, contact information for MAJCOM the eTools Lite Program Management Office can be found on the AFTOFST SharePoint.

11. System Identification Profile (SIP)

The SIP is produced as a by-product of being registered in eMASS. The current eTools Lite SIP can be obtained from eMASShttps://emass-airforce.csd.disa.mil/ or by request from the ISSM.

12. Plan of Actions and Milestones (POA&M)

The current eTools Lite POA&M is maintained in eMASS. The A4 format POA&M is provided as an artifact in eMASS or can be requested from the System ISSM or AF ELMS Project Office. The eTools Lite Mission Risk Assessment Briefing (MRAB) is used to document risk to the system and is maintained as a separate document which is available from the AF ELMS Project Office or eMASS.

13. Policy (AF, DoD)

- AFI 10-712 (Cyberspace Defense Analysis Operations and Notice and Consent Process)
- AFI 17-101 (Risk Management Framework for Air Force Information Technology)
- AFI 17-110 (Information Technology Portfolio Management and Capital Planning and Investment Control)
- AFI 17-130 (Air Force Cybersecurity Program Management)
- AFI 21-101 (Aircraft and Equipment Maintenance Management)
- AFI 91-208 (Hazards of Electromagnetic Radiation to Ordinance (HERO) Certification and Management)
- AFI 23-111 (Management of Government Property in Possession of the Air Force)
- AFMAN 17-1203 (Information Technology Asset Management)
- AFMAN 17-1301 (Computer Security)
- AFMAN 17-2101 (Long-Haul Communications Management)
- CJCSI 6211.02D (Defense Information Systems Network Responsibilities)
- CJCSI 6510.01F (Information Assurance and Support for to Computer Network Defense)
- CNSS Directive No. 510 (Directive on the Use oF Mobile Devices in Secure Spaces)
- DoD Memorandum: Approval of Multi-Factor Authentication Alternatives - RSA and YubiKey
- DoDD 8100.02 (Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense Global Information Grid)
- DoDI 5200.08-R (Physical Security Program)
- DoDI 5200.48 (Controlled Unclassified Information)
- DoDI 5230.24 (Distribution Statements on Technical Documents)
- DoDI 8100.04 (DoD Unified Capabilities)
- DoDI 8010.01 (DODIN Transport)
- DoDI 8420.01 (Commercial Wireless Local-Area Network Devices, Systems, and Technologies)
- DoDI 8500.01 (Cybersecurity)
- DoDI 8510.01 (Risk Management Framework for Information Technology)
- DoDI 8520.03 (Identity Authentication for Information Systems)
- DoDI 8530.01 (Cybersecurity Activities Support to DoD Information Network Operations)
- DoDI 8551.01 (Ports, Protocols, and Services Management)

14. References and Resources

- Apple: Security Updates
- Apple: Platform Security
- Apple: Hosts and ports are required to use Apple products on enterprise networks
- AF Form 1297 (Temporary Issue Receipt)
- AF Form 4433 (US Air Force Unclassified Wireless Mobile Device User Agreement)
- DISA Privileged User Cybersecurity Responsibilities Training
- DISA Smartphone and Tablet Training

- Air Force Information Assurance Collaborative Environment
- Commercial Internet Service Provider Wiki
- AFTOFST SharePoint
- HERO Certified Ordinance
- Wing Cybersecurity Office Information Assurance and TEMPEST
- DoD Mobility User Portal
- DoD Application Vetting Environment
- National Information Assurance Partnership
- AF Software and Application Certification Assessments
- AF Evaluated Product List
- DoDIN Approved Products List
- USCYBERCOM Information Assurance Vulnerability Management
- AF ePublishing
- Cyber.mil
- Defense Technical Information Center
- Committee on National Security Systems
- eMASS
- Air Force Information Technology and NetCentric Acquisition Guide
- NIST Cryptographic Module Validation Program
- NIST SP 800-88r1 (Guidelines for Media Sanitization)
- NIST SP 800-163r1 (Vetting the Security of Mobile Applications)
- NIST SP 800-124r1 (Guidelines for Managing the Security of Mobile Devices in the Enterprise)
- NIST NCCoE Mobile Device Security
- MITRE ATT&CK Mobile Mitigations
- NVD national vulnerability database
- DoD RMF Knowledge Service - Air Force Workspace
- USA.GOV