***BY ORDER OF THE
SECRETARY OF THE AIR FORCE***

HEADQUARTERS OPERATING INSTRUCTION 33-4

17 JULY 2018

Communications and Information

HEADQUARTERS AIR FORCE INFORMATION MANAGEMENT AND COMPLIANCE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available digitally on the e-Publishing website at **http://www.e-publishing.af.mil/**. If you lack access, contact the OPR to obtain a copy.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/AAII

Certified by: SAF/AAI
(Mr Kent Chadrick)

Supersedes: HOI33-4, 11 January 2013

Pages: 26

This instruction implements Air Force Manual 17-1203, Information Technology (IT) Asset Management (ITAM), 19 Mar 2014, Incorporating Change 2, 7 March 2017 and other applicable Air Force Communications and Information related policy directives and instructions. This Instruction applies only to Headquarters Air Force (HAF) military, civilian, and contractor personnel within the National Capital Region (NCR), and contains procedures for developing and managing Information Management (IM) and Information Technology (IT) guidance. It is the primary HAF publication for approved and promulgated information management and information technology policy and guidance previously issued by memorandum. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the Air Force Form 847, Recommendation for Change of Publication; route Air Force Form 847s through appropriate chain of command. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual 33-363, Management of Records, and disposed of in accordance the Air Force Records Disposition Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS).

SUMMARY OF CHANGES

This instruction has been substantially revised and should be reviewed thoroughly. It is renamed HOI 33-4, Information Management and Compliance and divided into three main sections:

Information Resource Management (IRM) (original HOI 33-4 as amended). Includes new guidance on “One Person, One Computer”, "Managed Print Services (MPS) Implementation and “Data Management Policy.” Memorandums listed below are rescinded and content included in this section:

SAF/AA memorandum Headquarters Air Force (HAF) Video Teleconferencing (VTC) Systems Policy, 1 Sep 2015 (rescinded)

SAF/AA memorandum HAF Policy Memorandum on Commercial Mobile Devices (CMD), 29 Aug 2014 (rescinded)

SAF/AAI memorandum Headquarters Air Force (HAF) Printing Efficiency – New Printer Device Policy, 13 Dec 2012 (rescinded)

SAF/AAI memorandum Rescind Policy Memorandum on Email Storage Limits within HAF, 28 Nov 2012 and Establishment of Organizational Mailbox Procedures, dated 27 January 2014 (rescinded)

Acquiring Information Technology Capabilities and Services within the AFNCR (updates and incorporates content from superseded HOI 33-15, Acquiring Information Technology Capabilities and Services, 8 October 2015). This section provides procedures for HAF organizations acquiring Information Technology capabilities and services within the AFNCR network. It details responsibilities organizations have when requesting Information Technology capabilities to support operational requirements.

Portfolio Compliance (new content). This section implements a governance and management process to ensure HAF Portfolio Information Technology investments (i.e., assets) are consistent with the Air Force strategic vision, mission objectives, best business practices, and the approved enterprise architecture. It defines the roles and processes designated Information Technology Asset Representatives and the HAF Portfolio Managers use in preparing the necessary documentation to demonstrate compliance with relevant Information Technology laws, regulations, and policies.

Chapter 1

INFORMATION RESOURCE MANAGEMENT

1.1. Overview.

1.1.1. Information Resource Management is a process for managing information resources to accomplish the HAF's mission, managing both the information itself and related resources such as personnel, equipment, funds, and Information Technology (IT) (Office of Manpower and Budget Circular A-130). Central management of information resources presents numerous opportunities for spending and process efficiencies and provides a HAF-wide view and focus.

1.2. Responsibilities.

1.2.1. The responsibilities for developing official HAF guidance and procedures for information resource management are as follows.

1.2.1.1. Director, Information Management (SAF/AAI).

1.2.1.2. Provides guidance for and compliance of information resources management for the HAF.

1.2.1.3. Ensures resources are acquired and managed consistent with applicable Air Force policy and guidance, the Clinger-Cohen Act (CCA) of 1996, Government Performance and Results Act (GPRA) of 1993, and the Paperwork Reduction Act (PRA) of 1995.

1.2.1.4. Defines and implements the Information Technology portfolio management process for the HAF.

1.3. Information Technology Management Board Working Group (ITMB-WG).

1.3.1. Chaired by the Director, Information Management (SAF/AAI), consists of O-6 or GS-15 level members representing each HAF two-letter organization.

1.3.2. Working Group members support and deliberate on behalf of their two-letter.

1.4. Chief Information Officer Support Division (SAF/AAII).

1.4.1. Provides the core staff to manage the Director, Information Management (SAF/AAI) mission.

1.4.2. Coordinates guidance and procedures.

1.4.3. Promulgates approved guidance documents. All approved guidance and/or procedure documents will be accessible to the user community and will be incorporated into this or other appropriate Headquarters Operating Instructions during their review and update cycle.

1.4.4. Maintains Information Management related records.

1.5. 844th Communications Group (844 CG).

1.5.1. Functions as the HAF's Information Technology provider and systems integrator.

1.5.2. Ensures guidance is compliant and consistent with Air Force and HAF architecture, cybersecurity, interoperability, and supportability standards.

1.5.3. Evaluates and recommends the most effective methods to implement Information Resources Management guidance.

1.5.4. Evaluates and identifies risks associated with guidance and where necessary, implements risk-mitigating measures.

1.5.5. Assists in monitoring implementation of Information Resource Management guidance to ensure uniform compliance across the HAF.

1.6. Guidance for Organizations and Individual Users.

1.6.1. The following paragraphs incorporate coordinated and approved guidance that was previously promulgated by official memoranda and, in accordance with Air Force Instruction 33-360, Publications and Forms Management, memoranda are now officially rescinded and/or elements of them are incorporated into this publication.

1.6.2. One Person One Computer. Organizations will ensure assigned personnel have either one desktop, laptop or tablet computer per classification level. Organizational leadership with operational requirements for additional equipment may submit a waiver request on organizational letterhead signed by the unit commander or equivalent to the AFDW/A6X organizational e-mail box **usaf.jbanafw.afdw-staff.mbx.afdw-a6x-workflow@mail.mil** for approval. Compelling mission-based justification or reasonable accommodation waiver approval is required before the service provider can assign a second device for the same classification level, or a laptop in a different classification level.

1.6.3. Common Access Card (CAC) Login. It is mandatory for all HAF computer network user accounts login to be Department of Defense (DoD) Common Access Card (CAC) only. For executive staff members that require the ability to read a senior leader's encrypted email, two options are available: alternate soft certificate or utilizing a copy of the principal's encryption certificate.

1.6.4. Data Management.

1.6.4.1. Electronic Mail. All personal and organizational mailbox owners will declare and store official sent mail as records in the approved record repository. Remaining unofficial email will be deleted or moved to local storage (.pst files) on C: drives or onto Compact Disc/Digital Versatile Disc. Note: .pst is a file extension meaning personal storage, and is not permitted on HAF network shared storage, excluding the Record drive. The use of the Auto-Archiving capability is encouraged to periodically convert old emails to a .pst file and move to a local storage drive.

1.6.4.1.1. Email Storage Limits. Under the DoD Enterprise Email (DEE) construct, all electronic mail accounts (personal and organizational) will receive a warning message at 3.5 gigabytes advising they are getting close to the storage limit and advising account owners to reduce mailbox size. After reaching the storage limit of 4 gigabytes, the account will no longer be able to send email.

1.6.4.1.2. Organizational Mailboxes. In support of the Secretary of Defense's effort to improve the Department's efficiency while reducing costs, organizational mailbox use and costs must be kept at a minimum. The aggregate cost of unnecessary, unused, or under-used mailboxes represents an inefficiency. Organizational mailboxes will not be established without a mission-impacting statement submitted via StoreFront at **https://52tayz-ws-005v/kinetic/DisplayPage?name=Storefront_Home**.

1.6.4.1.3. Email Distribution Lists (DLs). Requests for distribution lists are submitted with mission-impacting justification via StoreFront at **https://52tayz-ws-005v/kinetic/DisplayPage?name=Storefront_Home**.

1.6.4.2. Shared Drive Space Management. Only declared official records and official files (including media, i.e., video, audio, and pictures) are permitted on shared drives. All unofficial files must be deleted. The 844th Communications Squadron will delete all files on the shared drives (R: drive excluded) not modified in three years or more and will repeat this process every six months.

1.6.4.3. Storage of Official Records and Files. In accordance with Air Force Manual 33-363, users should file electronic records using the approved Air Force Electronic Records Management (ERM) solution. In addition, Air Force Instruction 33-322, Records Management, defines what is and is not an official record. Users should consult with their Organization/ Unit Records point of contact (POC) to review both organizational and individual files and migrate all official records to their ERM file share location. The length of time files can remain is determined by the dispositions directed in the controlling Tables and Rules from the RDS in AFRIMS which are included in each office's inventory of records. ERM file size is determined by the specific mission of a given unit and can be increased as mission demands dictate. The 844 CG backs up the data contained on the ERM shared drives regularly. The ERM program is managed for the HAF by the Director, Information Management (SAF/AAI) Records Management office at (703) 693-6223, e-mail: **usaf.pentagon.saf-aa.mbx.haf-records-mgt-workflow@mail.mil**. Refer to AFGM to HOI 33-17, HAF Records Management Program, and the HAF Records Management Plan at: **https://cs2.eis.af.mil/sites/11841/hafrm/HAF%20RECORDS%20MANAGEMENT%20rm%20PLAN/Forms/AllItems.aspx**.

1.6.4.4. SharePoint. The Air Force National Capital Region (AFNCR) Collaborative Environment (ACE) is implemented by SharePoint 2013, and enables organizations and individual users a convenient way to temporarily store, update, collaborate, reduce the need to pass large email file attachments, and publish various types of administrative data. In accordance with OMB A130 and AFI 33-322, medium or high impact PII cannot be stored in SharePoint unless a data at rest encryption is enabled. The 844 CG backs up data contained on SharePoint regularly. Individuals are limited to 50 megabytes (MB) of storage in the "My Sites" folders of SharePoint. Organizations are limited to a baseline allocation of 100 gigabytes (GB) which can be increased if mission justification warrants the expansion. The maximum size of a file that a user may upload to a SharePoint site is 50 megabytes (MB). If a user needs to upload a file greater than 50 megabytes (MB), the user must contact the Communications Focal Point at (202) 767-8000. SharePoint will flag site administrators of data that has not been accessed in over a year. If data needs to be retained longer than one year, users will consult with their unit SharePoint administrators and/or 744CS/SCP at (301) 981-1045, email: **usaf.jbanafw.744-cs.mbx.744-cs-sharepoint-support-team@mail.mil**.

1.6.4.5. Individual Computer Storage. Users may also place working files and draft documents on their computer's internal hard drive (i.e. "My Documents" folder). Users who desire to use Microsoft Outlook personal folders (.psts) will map them to their internal hard drive. 844 CG does not back up files stored on individual computers.

1.6.4.6. External Hard Drive Storage and Use. Approval for use of external hard drives is held at the 83rd Network Operations Squadron and requires annual registration renewal. The 844 CG/ SCO facilitates and submits requests to the 83rd Client Security. The 844 CG/SCO tracks acceptance or denial of Data Loss Prevention (DLP) requests, and maintains a listing of users with approved external hard drive exceptions. Customers may contact 844CG/SCO at (240) 612-0880, e-mail: **usaf.jbanfw.844-cg.list.mla-844-cg-sco@mail.mil**.

1.6.4.7. Personally Identifying Information (PII) Protection. In accordance with Air Force Instruction 33-332, Air Force Privacy and Civil Liberties, users must ensure PII is properly safeguarded and only accessible to individuals with a valid official need to know in order to conduct daily operations. Refer to HOI 33-19, HAF Privacy Roles and Responsibilities.

1.6.4.8. Prohibited Files. Certain file types inherently present risk to the Air Force Networks. A list of these files types is found at **https://saf-aa.sharepoint.afncr.af.mil/HAF_IM/ciobb/HAF%20CIO%20Policies/Data%20Management/List%20of%20Unauthorized%20File%20Types.docx** . The 844 CG will employ tools to prevent these types of files from being uploaded to the platforms mentioned in this instruction. It is understood that certain organizations need some of these file types and exceptions can be made when mission dictates. Users can submit waiver requests via StoreFront at: **https://52tayz-ws-005v/kinetic/resources/includes/tzOffsetCheck.jsp**

1.6.5. Audio Video (AV)/Video Teleconferencing (VTC) Systems. Only HAF two-letter offices are authorized classified and unclassified AV/VTC. Organizations with new mission essential requirements must submit a request via StoreFront at **https://52tayz-ws-005v/kinetic/DisplayPage?name=Storefront_Home**. Requests will be processed through the Facility Space Executive Oversight Board (**usaf.pentagon.saf-aa.mbx.saf-aao-workflow@mail.mil**) for review and approval, and fulfilled using standard HAF AV/VTC equipment.

1.6.6. Service Levels and Support for Platinum, Gold, and Silver Customers. Changes to the HAF Platinum and Gold customer list (add to, remove from) are addressed as they occur by the customer's organization to SAF/AAII Workflow at **usaf.pentagon.saf-aa.mbx.saf-aaii-workflow@mail.mil**. SAF/AAII in turn ensures changes meet Platinum and Gold criteria, and engages the 844 CG as appropriate for update of elevated service status.

1.6.6.1. Platinum Customers: The Secretary of the Air Force, the Under Secretary the Air Force, the Chief of Staff, the Vice Chief of Staff, the Director of Staff, the Chief Master Sergeant of the Air Force, select Arnold Corridor staff, all 3-4 star Generals/Senior Executive Service equivalents, and other two-letter principals are platinum customers. The 844 CG is required to respond during core duty hours to trouble calls from platinum customers within 10 minutes and resolve the ticket within 4 hours.

1.6.6.2. Gold Customers: All 1-2 Star Generals/Senior Executive Services equivalents, up to two front office staff members per platinum customer, and select Arnold Corridor staff are on the gold list. The 844 CG is required to respond during core duty hours to trouble calls from gold customers within 4 hours and resolve the ticket within 8 hours.

1.6.6.3. Silver Customers: All remaining customers are on the silver list. The 844 CG is required to respond during core duty hours to trouble calls from silver customers within one duty day and resolve the ticket within two duty days.

1.6.7. Information Technology Services in Private Residences (not applicable to services in government owned residences).

1.6.7.1. Personnel having legal Command and Control (C2) authority may be authorized applicable circuits in their private residence under certain circumstances.

1.6.7.2. For those personnel who have C2 responsibilities, services such as broadband Internet access, official phone, and computer(s) can be provided to their private residence.

1.6.7.3. The 844 CG is the only authorized provider of government-furnished Information Technology support to residences. The request submitted via StoreFront at **https://52tayz-ws-005v/kinetic/DisplayPage?name=Storefront_Home** must be approved prior to submission at the two-letter level. Unit funding using a Government Purchase Card (GPC) is not authorized for procurement of telecommunications (including internet service) to private residences.

1.7. Commercial Mobile Devices (CMD).

1.7.1. The Defense Information Systems Agency's (DISA) DoD Mobility Unclassified Capability (DMUC) provides the enterprise infrastructure to allow government purchased mobile devices access to the network (e.g., Defense Enterprise Email). Under this framework, the HAF portfolio consists of cell/smart phones and tablets assigned to and funded by organizations. Mobile Wi-Fi hotspot devices will be available for situational mission required use from the 844 CG loaner pool. SAF/AAR will deduct funds before the initial distribution for the number of devices each organization maintains.

1.7.2. All mobile device requirements will continue to be approved at the Deputy two-letter level or higher for processing and may not be further delegated. Tablet devices are approved for two-letter Principals and Deputies only, at the cost for initial and recurring funding by the organization. The approval memorandum will be submitted via StoreFront at **https://52tayz-ws-005v/kinetic/DisplayPage?name=Storefront_Home** along with the organizational fund cite.

1.8. Managed Print Services.

1.8.1. Overview. Managed Print Services will enable spending visibility and control, metrics tracking, policy enforcement, device standardization, a unified support model, and application of the latest cyber security controls including support for DISA Security Technical Implementation Guide (STIGs) and Windows10. It replaces all print devices across the AFNCR including Non-Secure Internet Protocol Router (NIPR) and Secure Internet Protocol Router (SIPR) remote sites EXCEPT where an organization specifically funds and supports all facets of printing, including managing their print servers, print queues, and security. The contract also does not include any Top Secret print devices.

1.8.2. Services. All maintenance and consumable costs (including fuser, toner, maintenance kits, etc.) are included in the Managed Print Services contract. Paper is not included due to price fluctuation. Managed Print Services will standardize on a limited number of Multi-Functional Device (MFD) models with scanning and printing capabilities. The vendor will provide device training and on-site personnel specialized in maintenance and support including a single number to call for all print issues. Managed Print Services provides additional capabilities including secure printing/scanning (CAC based), on-demand printing, and print anywhere technology.

1.8.3. Funding. The Managed Print Services initiative will be funded by organizations based on the number of devices and capabilities required on each device. Funding will be executed using a consumption model. Print device metrics will be measured using software tools to ensure the environment maintains efficient printing and new requirements are evaluated against current usage.

1.8.4. Legacy Devices. All legacy devices will be removed from the network and turned in by 30 Sep 2018. Connecting non-Managed Print Services devices directly to workstations and the network will be prohibited via technical enforcement. All legacy print queues and print servers will be decommissioned. For tenants not migrating any print queues on 844 CG, servers must be migrated off and maintained by tenant Information Technology staff.

1.8.5. New Print Device Requirements. Any requirement for a new print device must be submitted via StoreFront. The AFNCR Requirement Review Board (RRB) will validate requests to determine if an existing device can fulfill the requirement. New procurements must be limited to mission essential requirements.

Chapter 2

ACQUIRING INFORMATION TECHNOLOGY CAPABILITIES AND SERVICES WITHIN THE AFNCR

2.1. The Information Technology Requirements Process.

2.1.1. The Information Technology requirements process enables organizations (users) to obtain capabilities and services with the assistance of the 844 CG and the Headquarters Air Force Information Management Office (SAF/AAI). The Director, Information Management (SAF/AAI) has compliance and implementation oversight responsibilities for the HAF AFNCR network. The process for all related requirements begins when a Customer identifies a need (in functional terms) that potentially requires a solution(s) involving Information Technology capabilities and services (see attachment 4). The Customer submits requirements using StoreFront at: **https://52tayz-ws-005v/kinetic/DisplayPage?name=Storefront_Home**. These capabilities and services are grouped in two categories: HAF enterprise-wide (centrally funded) and organization unique (user funded).

2.1.2. HAF enterprise-wide requirements are those currently supported by the Headquarters Air Force network (HAFNet) or the Air Force network (AFNet) as standard products and services, such as laptops/desktops and peripherals, secure and unsecure voice, infrastructure and communications, and standard enterprise software. These requirements will be satisfied using supported capabilities having no impact on Information Technology infrastructure, architecture, standards, or policies. They are funded by the Director, Information Management (SAF/AAI) and purchased/maintained by the 844 CG. When sufficient funding is not available, the Customer will provide funding for these purchases. Customer funded requirements may be processed directly by the 844 CG without the Director, Information Management (SAF/AAI) involvement.

2.1.3. Organization unique requirements are those Customer-funded capabilities used by a limited number of organizations to satisfy unique mission requirements. They are capabilities and/or services not currently part of the standard products and services supported by the HAFNet, AFNet, or DoD. Requirements that potentially involve servers or server-based applications are automatically categorized as organization unique requirements. These requirements must be evaluated for their potential impact on the networks' infrastructure, architecture, standards, and policies. Each requesting organization is responsible for funding the unique requirements and their sustainment.

2.1.4. All organization unique requirements require Director, Information Management (SAF/AAI) involvement and approval, and in some cases, may involve SAF CIO/A6 or their designee's approval. If these requirements are approved but not funded, they will be held pending funds sourcing for up to 30 days. Once funding is secured, approved solutions will be implemented and sustained by the 844 CG.

2.2. Responsibilities.

2.2.1. The Customer (requesting organization) shall identify its requirements in functional terms. The requirement statement must describe the needed capability, and not a solution or product. The requirement statement should indicate when a secure capability is required.

When necessary, include special requirements, such as accommodations for users with special needs, special operating conditions, manpower, training, and maintenance. If specific equipment is required, a justification must be provided.

2.2.2. The 844 CG, as the Information Technology provider and systems integrator, is responsible for ensuring solutions address architecture compliance, cybersecurity, interoperability and supportability, and maintenance standards. They are also responsible for the solution development, planning and implementation, and for maintenance of the implemented solution within the Information Management infrastructure.

2.2.3. The Headquarters Air Force Information Management Directorate (SAF/AAI) is responsible for ensuring that HQ USAF Information Management investments address DoD and Air Force standards for enterprise architecture, cybersecurity, interoperability and supportability, and maintenance. SAF CIO/A6 CCA compliance covers many aspects: management, investment, implementation, operations, information assurance (cybersecurity), and others. Compliance relies on the Information System Owners (ISO), Program Managers (PM), Authorizing Officials (AO), and System Operators to comply with established policies/guidelines and execution of roles/responsibilities to ensure Air Force is in compliance with the CCA. SAF/AAI wears multiple hats for HAF as ISO, PM, and AO.

2.2.4. The HAF Resources Directorate (SAF/AAR) provides final funding approvals and advocates for funding through the Air Force Corporate Structure.

2.2.5. The Information Technology Management Board Working Group (ITMB-WG). See paragraph 1.3.

2.3. Identifying Requirements, Coordination, and Processing.

2.3.1. The Information Management capabilities and services acquisition process starts when a Customer identifies a requirement to support their mission.

2.3.2. The Customer first determines if business/process re-engineering or other non-technical solutions will satisfy the requirement. In some instances, enterprise-wide capabilities may exist which support some, if not all, of the Customer's requirements. The 844 CG is available for assistance in understanding current capabilities.

2.3.3. If a HAF enterprise-wide capability is not available to address the requirement, the Customer can request the assistance of the 844CG to evaluate requirements and recommend a technical solution (organization unique).

2.3.3.1. Principal criteria for requirements approval should be: (1) mission required; (2) non-duplicative and cost effective; (3) significantly enhance mission outcomes; (4) satisfy a validated need for improvement. All investments (e.g., programming and/or budgeting for new capabilities, developmental evaluations, system modernization, and sustainment) must be requested via the StoreFront website at **https://52tayz-ws-005v/kinetic/DisplayPage?name=Storefront_Home**. This is true regardless of whether these requirements have been pre-approved for funding by the Air Force Corporate Structure, and include capabilities and services to be hosted outside the HAF. All Information Technology related requests must be coordinated via StoreFront, even if the 844 CG will not be providing the requested capabilities or services. This coordination must be accomplished prior to soliciting a contract, transferring funds for purchase, or making a purchase via a government purchase card. This must be done to ensure technical solutions address architectural, cybersecurity, interoperability, follow-on maintenance, and supportability standards.

2.3.4. Prior to assessing possible technical solutions, the 844 CG will validate and categorize the requirements as HAF enterprise-wide (including DoD or AFNet services) or organization unique based on the criteria outlined in paragraphs 2.1 and 2.2.

2.3.4.1. The 844 CG will involve the Director, Information Management (SAF/AAI) on all organization unique requirements to determine if these requirements comply with all laws, regulations, and policies including Air Force Instruction 10-601, Operational Capability Requirements Development.

2.3.4.2. SAF/AAII will assess and present recommendations to the Director, Information Management (SAF/AAI) for consideration. SAF/AAI will assess the requirement and will notify the Customer and the 844 CG of the final decision. Approved requirements are forwarded to the 844 CG to develop and implement a technical solution.

2.3.5. The 844 CG will process and implement all HAF funded requirements and all approved and funded organization unique requirements.

2.4. Developing a Technical Solution.

2.4.1. For unique and/or non-standard requirements, the 844 CG completes a Technical Assessment and Cost Estimate (TACE) for the Customer's approved requirement. If needed, they may request SAF/AAII assistance regarding policies, standards, and architecture compliance of potential solutions. The Customer has 30 days to review and fund or request changes to the Technical Assessment and Cost Estimate.

2.4.2. The Customer reviews the solution to ensure it satisfies the requirement and addresses any outstanding issues with the 844 CG project manager. If modifications are needed to the selected solution, 844 CG will ensure modifications have no impact to the Air Force Network and the Headquarters Air Force infrastructure, architecture, standards, and policies.

2.5. Implementing the Technical Solution.

2.5.1. The 844 CG will take the required steps to meet HAF enterprise-wide requirements.

2.5.2. The 844 CG will develop a plan to implement approved organization unique and/or nonstandard requirements. This plan and other necessary documents will follow all required standards, policies, and architectures. The 844 CG project manager will contact SAF/AAII if there are potential issues/concerns.

2.5.3. SAF/AAII will review these documents for standards, policies, and architecture compliance; and will cross-reference them with current capabilities to avoid potential duplication. If changes are required, SAF/AAII will forward its findings to the 844 CG project manager.

2.5.4. Upon Director, Information Management (SAF/AAI) approval, and Customer fund commitment (transferred), the 844 CG project manager will proceed to the implementation of an accepted solution based on compliance with all policies, standards, and architecture.

2.6. Post Implementation.

2.6.1. Upon completion of the implementation of the approved solution, the 844 CG will notify the Customer that the solution is in production and available for use.

2.6.2. Using documented performance measures and expected improvements, the Customer will validate that deliverables meet the requirement. If the expected features and functionalities are not delivered by the final solution, the Customer will contact the 844 CG for resolution.

2.6.3. Resolution of issues on systems/solutions not delivered or managed by the 844 CG will require the Customer, with 844 CG involvement, to contact the respective vendor/integrator or organization.

2.7. Funding.

2.7.1. Funding Sources. Funding sources for Information Technology solutions include the Customer, the HAF enterprise, and the lead command/component in the case of Service or Department-wide programs. Requirements may also be endorsed by the Director, Information Management (SAF/AAI) and compete for funding through the Director, Resources (SAF/AAR) to the Air Force Corporate Structure.

2.7.2. User-funded Requirements. Upon approval of the requirement and associated solution, funds are transferred to the 844 CG to purchase the solution (product and/or service). Prior to acquisition, the Customer will ensure funds are available and approved. In some cases, the Customer will be responsible for the yearly sustainment cost and must ensure out-year funds are available and approved.

2.7.3. Funds Hold. If funds are not available for the solution and the 844 CG services do not cover the requirement, the Customer is responsible for the funding with the requirement being placed on funds hold. Generally, funding must be identified within 30 days or the requirement will be closed. The 844 CG project manager will notify the Customer that the requirement is being closed before reaching the 30-day limit. If funds become available after the requirement is closed, the Customer can resubmit the requirement, and a new tracking number will be assigned.

Chapter 3

PORTFOLIO COMPLIANCE

3.1. Overview and Background.

3.1.1. To manage a diverse Air Force Information Technology Portfolio, the Air Force Chief Information Officer (SAF CIO/A6) uses a decentralized Information Technology Portfolio Owner approach to implement Air Force Instruction 17-110, Information Technology Portfolio Management and Capital Planning and Investment Control. Information Technology portfolios are segmented by Major Command, Direct Reporting Units, Functional organization, and the HAF. The Director, Information Management (SAF/AAI) serves as the HAF Chief Information Officer and Headquarters Air Force Portfolio owner and oversees an Information Technology portfolio for those Headquarters Air Force two-letter organizations not designated by SAF CIO/A6 as a Chief Information Officer/Portfolio Owner.

3.1.2. The Director, Information Management (SAF/AAI) portfolio guidance is intended to accomplish the following objectives:

3.1.2.1. Provide Asset Representatives and the Portfolio teams with a comprehensive overview of the information required to certify compliance on their systems and actions to maintain certification.

3.1.2.2. Ensure Asset Representatives and the Portfolio teams understand the different categories of compliance, the intent of the compliance requirements, and the tools/templates/formats used to provide the information for certification.

3.1.2.3. Provide sufficient context, so that Asset Representatives and the Portfolio teams can successfully navigate all available policy, regulation, and guidance related to the certification process.

3.1.2.4. Establish a governance process designed to ensure HAF Portfolio Information Technology investments are consistent and compliant with the Air Force strategic vision, mission objectives, best business practices, cybersecurity, and the approved enterprise architecture.

3.1.2.5. Enable Asset Representatives and their Portfolio teams to control new Information Technology investments and evaluate existing systems to identify and eliminate duplication and functional overlap.

3.1.2.6. Examine and account for Information Technology investments across the enterprise, promote standardization of capabilities where practical, and eliminate duplication of functions and capabilities within systems.

3.1.3. Portfolio Management.

3.1.3.1. Overview. Portfolio Management is the management of selected groupings of investments through integrated strategic planning, architecture, measures of performance, risk-management techniques, and transition plans.

3.1.3.2. Mission and Vision. To fully leverage information technology resources through the entire lifecycle, from research/initialization to asset decommissioning:

synchronizing milestones and dependencies while measuring performance to optimize, drive, and manage investment decisions. Portfolio Management identifies the best mix of investments to maximize portfolio performance through analysis, selection, and control of critical portfolio capabilities and associated investments, to achieve DoD and Air Force organizational goals and objectives.

3.1.3.3. Objective. To align Information Technology investments and integrate architectures, enabling informed decisions to stop, slow, maintain, and accelerate funding in support of the Department of Defense and Air Force enterprise strategic vision. Portfolio Management ensures Department of Defense compliance and Information Technology certification requirements are adhered to, and identifies redundant and inefficient systems. This is accomplished by establishing performance measures and identifying and resolving fielding/migration timelines to facilitate improved program execution.

3.1.3.4. Applicability and Scope. Portfolio Management applies to all Air Force organizations that develop, review, approve, manage or fund Headquarters Air Force Information Technology investments, including Major Command Information Technology investments/requirements that align with Headquarters Air Force functions. DoD compliance and Information Technology certification requirements are mandatory, except when statutory requirements or DoD or Joint Staff directives override.

3.1.4. Roles and Responsibilities.

3.1.4.1. HAF Portfolio Manager, Chief Information Officer Support Division (SAF/AAII):

3.1.4.1.1. Develops Information Technology Portfolio investment strategy and objectives, and is responsible for reporting on HAF Portfolio investments to the appropriate senior governance forums. Performs the functional portfolio duties for the Defense Security Enterprise Portfolio. Acts as the liaison between SAF CIO/A6, functional portfolio sponsors/proponents, Major Command Portfolio Managers, and Asset Representatives.

3.1.4.1.2. Assists Asset Representatives with registering HAF Information Technology assets in the official Air Force Information Technology registration systems:

- Information Technology Investment Portfolio Suite (ITIPS): is the Air Force's officially-designated Information Technology data repository used to collect Information Technology system information at the Air Force level for both internal compliance and reporting to DoD and Office of the Secretary of Defense. See the Portfolio Wiki for the Air Force and DoD data repository relationships: **https://cs2.eis.af.mil/sites/11841/HAF%20Portfolio%20Management%20Wiki/ITIPS.aspx**.
- Enterprise Mission Assurance Support Service (eMASS): the Risk Management Framework business process tool for Assess and Authorize (A&A) activities.

3.1.4.1.3. Ensures Information Technology asset development is reviewed for enterprise architecture compliance.

3.1.4.1.4. Ensures and certifies HAF and Defense Security Enterprise functional portfolio assets are reviewed at least annually.

3.1.4.1.5. Conducts periodic portfolio reviews for redundancy/duplication.

3.1.4.1.6. Assists with Asset Representative appointment and initial/bi-annual refresher training (reference attachments 1 and 2).

3.1.4.1.7. Ensures all Information Technology governance and compliance requirements are met. Publishes supporting compliance policy and guidance as needed, and disseminates requirements to Headquarters Air Force and Defense Security Enterprise functional portfolio Asset Representatives.

3.1.4.1.8. Certifies to the Air Force Chief Information Officer completion of annual review on all systems in the HAF and Defense Security Enterprise functional portfolios.

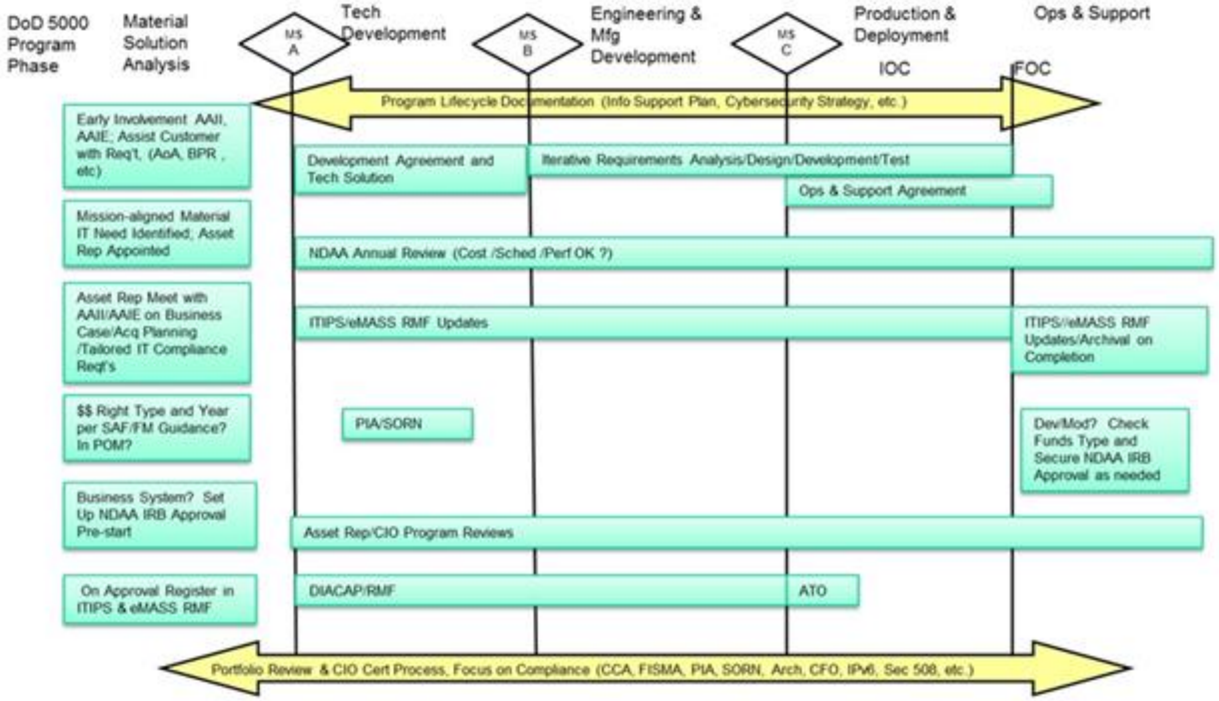
3.1.4.1.9. Provides recommendations on unfunded Information Technology submissions.

3.1.4.1.10. Submits National Defense Authorization Act (NDAA) certification packages to Air Force Chief Information Officer (SAF CIO/A6) for review.

3.1.4.1.11. The HAF Information Technology Portfolio area of responsibility includes organizations without a two-letter functional Chief Information Officer. Supported organizations are at: **https://cs2.eis.af.mil/sites/11841/HAF%20Portfolio%20Management%20Wiki/Home.aspx**.

3.1.4.2. Program Management (Information System Owner/Asset Representative) Responsibilities: Air Force Instruction 63-101/20-101, Integrated Life Cycle Management, paragraph 1.5.1, requires Air Force programs have a clear and unambiguous governance chain of authority, including a designated Program Manager to manage cost, schedule and performance. For the purpose of Portfolio Management, the Asset Representative role is filled by the Program Manager function for Acquisition programs. For non-Acquisition programs, the Asset Representative performs duties equivalent to the Program Manager function. Figure 3.1 depicts notional management activities an Asset Representative will be involved in during an Information Technology asset’s lifecycle. These activities are covered in more detail in the following paragraphs. Air Force Instruction 63-101/20-101, Chapter 8, outlines an important set of management responsibilities for Information Technology systems. Additional information on compliance activities can be found at: **https://cs2.eis.af.mil/sites/11841/SiteAssets/HAF%20Portfolio%20Management%20Wiki/**.

Figure 3.1. Portfolio Engagement Flow.


DoD 5000 Program Phase
Material Solution Analysis
MS A
Tech Development
MS B
Engineering & Mfg Development
MS C
Production & Deployment
Ops & Support
IOC
FOC
Program Lifecycle Documentation (Info Support Plan, Cybersecurity Strategy, etc.)
Early Involvement AAII, AAIE; Assist Customer with Req't, (AoA, BPR , etc)
Mission-aligned Material IT Need Identified; Asset Rep Appointed
Asset Rep Meet with AAII/AAIE on Business Case/Acq Planning /Tailored IT Compliance Reqt's
$$ Right Type and Year per SAF/FM Guidance? In POM?
Business System? Set Up NDAA IRB Approval Pre-start
On Approval Register in ITIPS & eMASS RMF
Development Agreement and Tech Solution
Iterative Requirements Analysis/Design/Development/Test
Ops & Support Agreement
NDAA Annual Review (Cost /Sched /Perf OK ?)
ITIPS/eMASS RMF Updates
ITIPS//eMASS RMF Updates/Archival on Completion
PIA/SORN
Dev/Mod? Check Funds Type and Secure NDAA IRB Approval as needed
Asset Rep/CIO Program Reviews
DIACAP/RMF
ATO
Portfolio Review & CIO Cert Process, Focus on Compliance (CCA, FISMA, PIA, SORN, Arch, CFO, IPv6, Sec 508, etc.)

3.1.4.2.1. Asset Representatives are responsible for management of system cost, schedule, performance, funding, system registration, and generation of information for multiple compliance items. Air Force Instruction 63-101/20-101, Chapter 8, outlines an important set of management responsibilities for Information Technology systems.

3.1.4.2.2. Asset Representatives will be appointed and complete initial and bi-annual refresher training, which includes:

• Initial Training: hands-on training sessions with the Portfolio Team to include specialized training on use of ITIPS and eMASS.
• Refresher Training: Bi-annual attendance at SAF/AAII Portfolio assessments (all asset representatives).

3.1.4.2.3. Asset Representatives are responsible for completing compliance activities and for participating in bi-annual Portfolio assessments per instructions provided by the Headquarters Air Force Portfolio Management team.

3.1.4.2.4. Asset Representatives are responsible for ITIPS and eMASS for compliance and support of Air Force Information Technology Portfolio Management processes.

3.1.4.2.4.1. Asset Representatives will register their Information Technology assets, including National Security Systems (NSS), in ITIPS for registration are provided on the Portfolio Wiki: **https://cs2.eis.af.mil/sites/11841/SiteAssets/HAF%20Portfolio%20Management%20Wiki/**

3.1.4.2.4.2. Asset Representatives will also register their assets in eMASS if required for cybersecurity compliance (reference Air Force Instruction 17-101, Risk Management Framework (RMF) for Air Force Information Technology). Registration instructions and responsibilities are detailed on the Portfolio Wiki, **https://cs2.eis.af.mil/sites/11841/SiteAssets/HAF%20Portfolio%20Management%20Wiki/**

3.1.4.2.5. Asset Representatives will ensure continuity of operations for data surety have been evaluated and contingency planning is documented for their asset(s). In addition, the users of the asset are able to execute the contingency plan if their asset becomes unavailable due to system malfunction, outages, etc.

3.1.4.2.6. Asset Representatives will ensure NDAA certification is obtained for Defense Business Systems. The Asset Representative obtains certification approved by the Portfolio Owner, SAF/MG, or the Defense Business Committee. For current Fiscal Year thresholds, see the Portfolio Wiki: **https://cs2.eis.af.mil/sites/11841/SiteAssets/HAF%20Portfolio%20Management%20Wiki/**

The Asset Representative will comply with NDAA certification Delegation Levels for Defense Business Systems. Asset Representatives will work with assigned Air Force Organization Execution Plan representatives in their conduct of annual reviews of all Defense Business Systems spending $1Million or greater across the Future Years Defense Program. Asset Representatives managing Defense Business Systems will work with the Portfolio Team to identify their functional Organization Execution Plan lead for initial certification and annual review (reference Air Force Manual 63-144, Defense Business System Life Cycle Management).

3.1.4.2.7. Asset Representatives are responsible for development of the program cybersecurity to ensure compliance with the statutory requirements of United States Code Title 40/Clinger-Cohen Act and related legislation, as implemented by Department of Defense Instruction 5000.02, Operation of the Defense Acquisition System.

3.2. Portfolio Management Contacts.

3.2.1. For most compliance issues, ITIPS and eMASS registration, NDAA certification, cybersecurity, and other items not listed below: **usaf.pentagon.saf-aa.mbx.haf-piaso@mail.mil**.

3.2.2. Privacy Act, System of Record Notice (SORN), Civil Liberties, and Records Management: **usaf.pentagon.saf-aa.mbx.haf-privacy-office@mail.mil** or **usaf.pentagon.saf-aa.mbx.haf-records-mgt-workflow@mail.mil**.

3.2.3. For other HAF organizations with a Functional Chief Information Officer contact the Portfolio Manager of that organization.

KENT E. CHADRICK, SES
Director, Information Management

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 10-601, Operational Capability Requirements Development, 6 Nov 2013

AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT), 2 Feb 2017

AFI 17-110, Information Technology Portfolio Management and Capital Planning and Investment Control, 23 Dec 2008

AFI 33-322, Records Management Program, 25 May 2017

AFI 33-332, Air Force Privacy and Civil Liberties, 17 November 2016

AFI 63-101/20-101, Integrated Life Cycle Management, 9 May 2017

AFMAN 17-1203, Information Technology (IT) Asset Management (ITAM), 19 Mar 2014, Incorporating Change 2, 7 March 2017

AFMAN 33-363, Management of Records, 1 Mar 2008

AFMAN 63-144, Defense Business System Life Cycle Management, 31 Mar 2016

Department of Defense Instruction 5000.02, Operation of the Defense Acquisition System, 7 Jan 2015

Information Technology Management Reform Act of 1996 (ITMRA), also known as the Clinger-Cohen Act of 1996 -- DoD Requirements for Clinger-Cohen Act (CCA) implementation

Office of Manpower and Budget Circular A-130, Management of Federal Information Resources (Transmittal Memorandum No. 4)

Paperwork Reduction Act (PRA) of 1995

Prescribed Forms

No Prescribed Forms

Adopted Forms

Air Force Form 847, Recommendation for Change of Publication

Abbreviations and Acronyms

844 CG—844th Communications Group

844 CS—844th Communications Squadron

A&A—Assess and Authorize

ACE—AFNCR Collaborative Environment

AF—Air Force

AF CIO—Air Force Chief Information Officer

AFI—Air Force Instruction

AFNCR—Air Force National Capital Region

AFNet—Air Force Network

AV—Audio Video

C2—Command and Control

CAC—Common Access Card

CCA - Clinger—Cohen Act of 1996

CIO—Chief Information Officer

CMD—Commercial Mobile Device

DEE—Defense Enterprise Email

DISA—Defense Information Systems Agency

DL—Distribution List

DLP—Data Loss Prevention

DMUC—DoD Mobility Unclassified Capability

DoD—Department of Defense

eMASS—Enterprise Mission Assurance Support Service

FISMA—Federal Information Security Management Act

GPC—Government Purchase Card

HAF—Headquarters Air Force

HAFNet—Headquarters Air Force Network

HOI—Headquarters Operating Instruction

IM—Information Management

IRM—Information Resources Management

IT—Information Technology

ITIPS—Information Technology Investment Portfolio Suite

ITMB WG—Information Technology Management Board Working Group

ITMRA—Information Technology Management Reform Act of 1996

MAJCOM—Major Command

MFD – Multi—Functional Device

MPS—Managed Print Services

NDAA—National Defense Authorization Act

NIPR – Non—Secure Internet Protocol Router

NSS—National Security System

OPR—Office of Primary Responsibility

PCA—Permanent Change of Address

PCS—Permenent Change of Station

PfM—Portfolio Management

PII—Personally Identifiable Information

PM—Program Manager

PRA—Paperwork Reduction Act of 1995

RMF—Risk Management Framework

RRB—Requirement Review Board

SAF/AA—Office of the Administrative Assistant to the Secretary of the Air Force

SAF/AAI—Headquarters Air Force Information Management Directorate, Office of the Headquarters Air Force Chief Information Officer

SAF/AAII—Headquarters Air Force Chief Information Officer Support Division

SES—Senior Executive Service

SIPR—Secure Internet Protocol Router

SORN—System of Records Notice

SSN—Social Security Number

STIG—Security Technical Implementation Guide

TACE—Technical Assessment and Cost Estimate

VTC—Video Teleconferencing

Terms

Asset Representative—is the individual responsible for management of cost, schedule, performance and compliance aspects of an Information Technology (IT) application. While Asset Representatives generally manage smaller Information Technology assets, the management functions are synonymous with Program/Project manager, applicable to larger Information Technology systems, programs and projects.

Chief Information Officer—s the person responsible for information management, information technology, and computer systems that support enterprise goals.

Cybersecurity—is the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Enterprise Mission Assurance Support Service—is a web-based Government off-the-shelf (GOTS) solution that automates a broad range of services for comprehensive, fully-integrated cybersecurity management, including controls scorecard measurement, dashboard reporting, and the generation of Risk Management Framework (RMF) package reports for Department of Defense (DoD) Information Technology (IT). Enterprise Mission Assurance Support Service (eMASS) provides an integrated suite of authorization capabilities and prevents cyber-attacks by establishing strict process control mechanisms for obtaining authority to connect information systems to Department of Defense networks.

Enterprise—wide Products and Services-include all sustainment services, and all standard products and services (Information Technology capabilities) approved for use across the HAF; these may include DoD or Air Force (AFNet) provided products and services.

Functionally Unique Products and Services include all sustainment services, and all products and services (IT Capabilities) that must be satisfied by a unique IT capability used by only one or a limited number of HAF 2-Ltr offices.

Headquarters, Department of the Air Force—in the context of this Operating Instruction encompasses Secretariat and Air Staff organizations to include offices of the Secretary of the Air Force, the Undersecretary of the Air Force, Chief of Staff of the Air Force, Vice Chief of Staff of the Air Force, and Assistant to the Vice Chief of Staff of the Air Force.

Headquarters Operating Instruction—is a directive publication similar to a field publication (Major Command level) as it does not apply across the Air Force, and assigns responsibilities, directs actions, and prescribes procedures within a Headquarters (in this case Headquarters Air Force).

Information Resources Management—is the process of managing information resources to accomplish the agency mission. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and Information Technology (Office of Manpower and Budget Circular A-130).

Information Technology Investment Portfolio Suite—is the Air Force Information Technology Portfolio Management system of record containing a current inventory of initiatives, systems, and system-related data and is used for internal management and oversight as well as to provide information to external sources to satisfy statutory and regulatory requirements.

Portfolio Management—is the work of finding the best way to support Air Force business processes with the right combination of Information Technology services. Portfolio Management requires a clear understanding of strategic goals in order to relate decisions and expenditures to organizational value. Value is driven by applying Information Technology to the business goals of the organization. Furthermore, effective Portfolio Management requires an "across the board" application of standards for decision making on where Information Technology investments will be made.

Risk Management Framework—is the “common information security framework” for the federal government and its contractors. The stated goals are to improve information security, strengthen risk management processes and encourage reciprocity among federal agencies. Through implementation of the Risk Management Framework, federal agencies can achieve compliance with policy directives such as the Federal Information Security Management Act (FISMA), and Office of Management and Budget (OMB) Circular A-130. Risk Management Framework effectively transforms traditional Certification and Accreditation (C&A) programs into a six-step life cycle process consisting of: 1. Categorization of information systems, 2.

Selection of security controls, 3. Implementation of security controls, 4. Assessment of security controls, 5. Authorization of information systems and 6. Monitoring of security controls.

Storefront—is a web-based interface between the Customer and the Provider.

Attachment 2

SAMPLE APPOINTMENT LETTER OF INFORMATION TECHNOLOGY ASSET REPRESENTATIVES

(Date)

MEMORANDUM FOR SAF/AAII (Information Technology Portfolio Manager)

FROM: (Sender Two-Letter Organization)

SUBJECT: Appointment of Information Technology (IT) Asset Representative for [Investment(s)]

The individuals listed below are appointed as IT Asset Representatives for [IT Investment(s)]. Asset Representatives will monitor their applications for all assigned investments and perform duties in accordance with AFI 17-110, Air Force Information Technology Portfolio Management and IT Investment Review and HOI 33-4, Headquarters Air Force Information Management and Compliance.

PRIMARY NAME:
RANK/GRADE:
OFFICE SYMBOL:
DUTY PHONE:
E-MAIL:

ALTERNATE NAME:
RANK/GRADE:
OFFICE SYMBOL:
DUTY PHONE:
E-MAIL:

Appointed Asset Representatives will complete training 60 days from the date of this letter and will contact SAF/AAII 90 days prior to any Office of Primary Responsibility changes (ex. Permanent Change of Station (PCS), Permanent Change of Address (PCA), retirement, etc.).

Signature Block
(GS-15/06 or higher in the appointee’s organization)

Attachment 3

CERTIFICATION STATEMENT

CERTIFICATION OF INITIAL/ANNUAL REFRESHER TRAINING
HEADQUARTERS AIR FORCE PORTFOLIO ASSET REPRESENTATIVE

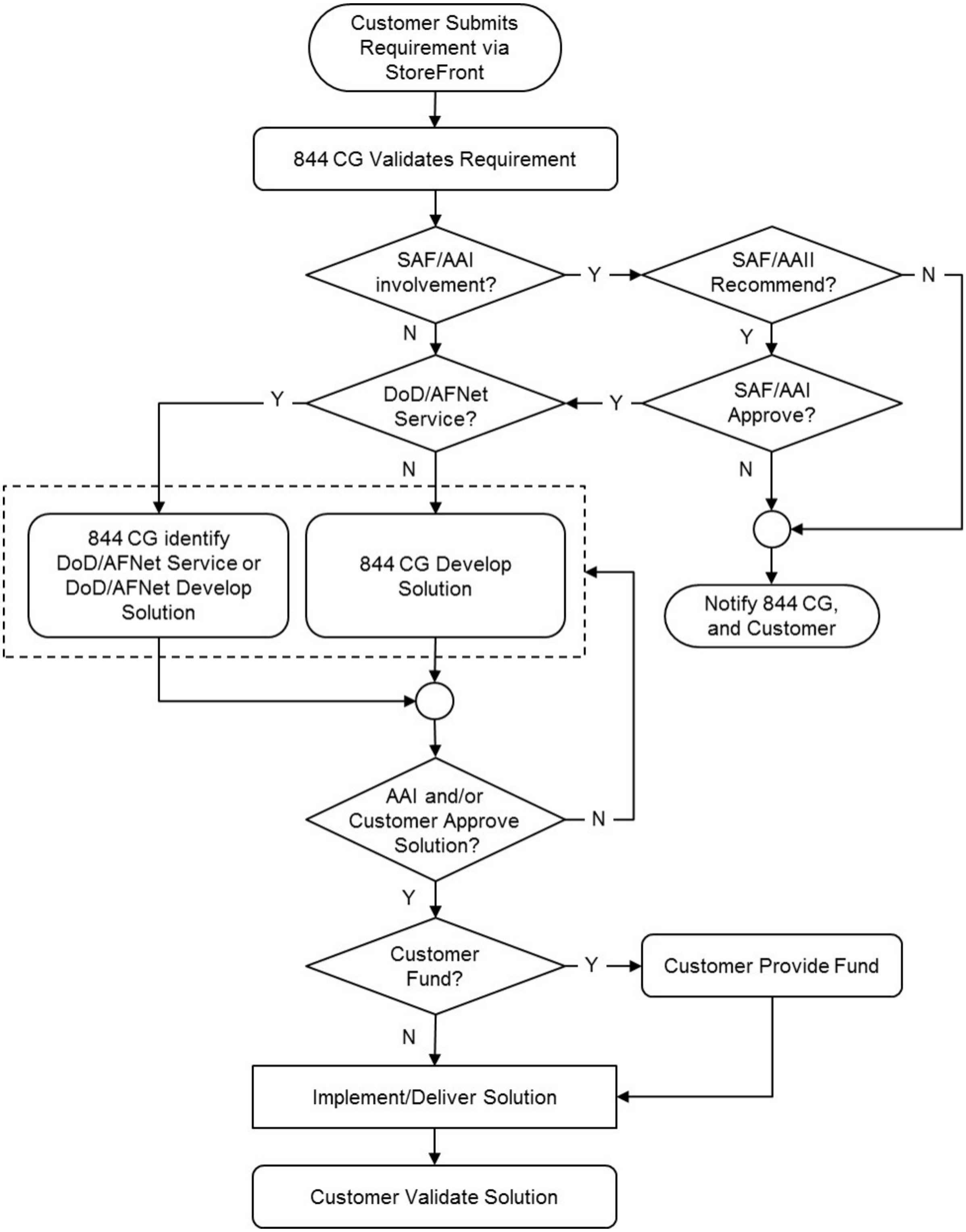
This is to certify that I have received initial/annual refresher training on my Headquarters Air Force Information Technology Asset management responsibilities in accordance with Headquarters Operating Instruction 33-4.

______________________________ (Signature)	______________________________ (Print Name)
______________________________ (Date)	______________________________ (Office)

Attachment 4

HAF IT CAPABILITIES AND SERVICE ACQUISITION PROCESS

Figure A4.1. HAF IT Capabilities and Service Acquisition Process.


Customer Submits Requirement via StoreFront
844 CG Validates Requirement
SAF/AAI involvement?
Y
SAF/AAII Recommend?
N
N
Y
Y
DoD/AFNet Service?
Y
SAF/AAI Approve?
N
N
844 CG identify DoD/AFNet Service or DoD/AFNet Develop Solution
844 CG Develop Solution
Notify 844 CG, and Customer
AAI and/or Customer Approve Solution?
N
Y
Customer Fund?
Y
Customer Provide Fund
N
Implement/Deliver Solution
Customer Validate Solution