# DEPARTMENT OF THE AIR FORCE
### WASHINGTON, DC

MEMORANDUM FOR AUTHORIZING OFFICIALS

SUBJECT:  Automated Remediation and Asset Discovery (ARAD) on PEO/PMO systems

REFERENCES: (a) HAF Mission Directive 1-26
             (b) AFI 17-101 Risk Management Framework for Information Technology

1.  To provide mission assurance for the Air Force core missions we must leverage enterprise-wide tools to maintain operational advantage.  Separate enclaves running different tools that do not connect to each other or provide easy access to the data at the enterprise level are not effective.  Accordingly, I consider the connection of any IT investment to our networks without Automated Remediation and Asset Discovery (ARAD) to be high risk.

2.  Deploying ARAD establishes real-time visibility into baseline configurations and vulnerability status for Information Assurance Vulnerability Management compliance at the enterprise level.  ARAD will also enable mission owners to monitor their systems and implement change management and configuration control processes.

3.  Pursuant to references (a) and (b), I am directing Authorizing Officials to ensure IT investments in their portfolio have executed the ARAD capability immediately where possible, but no later than 31 May 2017.  If mission requirements necessitate a temporary waiver after 1 June 2017, the waiver authority is the Air Force CIO and the waiver will be submitted through the Air Force CISO.

4.  This applies to all AF Information Technology, Operational Technology, and Platform Information Technology where there is an ARAD agent for the operating system.  This guidance currently applies to all systems that connect to NIPRNET and will be applied to all systems connecting to other networks such as SIPRNET once the ARAD infrastructure is in place on those systems.

5.  My OPR for this action is Lt Col John Bidol, john.a.bidol.mil@mail.mil, (703) 695-6802.


WILLIAM J. BENDER, Lt Gen, USAF
Chief, Information Dominance and
 Chief Information Officer