DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

AFI17-101_AFGM2016-01

28 October 2016

MEMORANDUM FOR DISTRIBUTION C
MAJCOMs/FOAs/DRUs

FROM: SAF/CIO A6
1800 Air Force Pentagon
Washington, DC 20330-1800

SUBJECT: Air Force Guidance Memorandum to AFI33-210 *AIR FORCE CERTIFICATION AND ACCREDITATION (C&A) PROGRAM (AFCAP)*

By Order of the Secretary of the Air Force, this Air Force Guidance Memorandum immediately AFI33-210 *Air Force Certification and Accreditation (C&A) Program (AFCAP),* 2 Oct 2014. Compliance with this Memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications, the information herein prevails, in accordance with (IAW) AFI 33-360, *Publications and Forms Management*. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

As a result of the publication of AF Policy Directive (AFPD) 17-1, *Information Dominance and Cyberspace Governance and Management*, which supersedes AFPD 33-2, *Information Assurance (IA) Program*, dated 3 August 2011, AFI33-210 is hereby renumbered as AFI 17-101. This Memorandum is a renumbering of AFI33-210 only; the title and content remain unchanged. I hereby direct the Office of Primary Responsibility (OPR) for AFI33-210 to conduct a special review in accordance with AFI33-360 to align its content with AFPD17-1. This will result in a rewrite or rescind action of AFI33-210.

This Memorandum becomes void after one year has elapsed from the date of this Memorandum, or upon rescinding or rewrite of AFI33-210, whichever is earlier**.**

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

BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-210

23 DECEMBER 2008

Incorporating Change 1, 2 October 2014

Communications and Information

AIR FORCE CERTIFICATION AND ACCREDITATION(C&A) PROGRAM (AFCAP)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-publishing.af.mil.**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/XCPP

Certified by: SAF/XCP-2
(Brig Gen Ronnie Hawkins)

Pages: 40

This Air Force Instruction (AFI) implements DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, 12 March 2014, and associated processes outlined on the RMF Knowledge Service, for authorizing the operation of Air Force Information Systems (ISs) consistent with the Federal Information Security Management Act (FISMA), DoD Instruction 8500.01, Cybersecurity, 14 March 2014, and DoD Directive 8000.01, Management of the Department of Defense Information Enterprise, February 10, 2009. Additionally, this AFI implements the approval to connect process for DoD information systems consistent with Air Force Policy Directive (AFPD) 33-2, *Information Assurance (IA) Program* (3 Aug 11); SAF memo, *Implementation of Information Technology Lean Reengineering Improvements* (28 Nov 05); AF-CIO memo, *IT System Certification and Accreditation Plan of Action and Milestones (POA&M)* (9 Dec 04); SAF/XC memo, *Designated Approval Authority (DAA) for the Air Force Provisioned Portion of the Global Information Grid* (5 Aug 05); and SAF/XC memo, *Accountability of Designated Approval Authority (DAA) and Program Manager (PM) for System Security* (8 Nov 05). This instruction applies to all Air Force military, civilian, and contractor personnel under contract by DoD who develop, acquire, deliver, use, operate, or manage Air Force information systems, including the Air National Guard (ANG) and Air Force Reserve Command. The term Major Command (MAJCOM), when used in this publication, includes Field Operating Agencies (FOA) and Direct Reporting Units (DRU). Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule located at **https://afrims.amc.af.mil/**. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR)

using the AF IMT 847, *Recommendation for Change of Publication*; route AF IMT 847s from the field through the appropriate functional's chain of command.

Chapter 1

GENERAL INFORMATION

1.1. Purpose. This AFI implements DIACAP for authorizing the operation of Air Force ISs consistent with federal, DoD, and Air Force policies. This AFI along with the *IT Lean Re-engineering Guidebook* will provide the basic framework of the C&A process, the AF connection approval process, and procedures for individual task accomplishment. Compliance with this AFI supports the following tenets:

1.1.1. Standardized Air Force C&A approach to meet DoD requirements.

1.1.2. Dynamic process capable of supporting all types of ISs.

1.1.3. Development of secure, interoperable, supportable, sustainable, and useable ISs.

1.1.4. Management of the IA posture of DoD information systems across the Air Force-provisioned portion of the Global Information Grid (AF-GIG).

1.2. Applicability. This AFI is applicable and mandatory for the development and operation of all Air Force ISs, and applications with the exception of those systems indicated in paragraph 2.2. below.

1.2.1. AF sponsors of Guest ISs (formerly known as Non-Air Force ISs) seeking connection to the AF-GIG must ensure the Air Force connection approval requirement is followed. This includes ANG ISs wholly funded by ANG.

1.2.2. While the Air Force accepts other service, agency, or department C&A documentation, such C&A documentation must be reviewed to ensure that any detrimental impacts on the networks supporting Air Force warfighters are unlikely to occur and that appropriate Ports, Protocols, and Services (PPS) are available to the IS seeking connection.

1.2.3. Joint organizations and Joint bases hosted by the Air Force with Air Force receiving accreditation from the other services will follow the connection approval process of this publication. Joint organizations and Joint bases hosted by the Air Force with Air Force providing C&A services will follow the AFCAP in its entirety.

1.3. Objectives. To ensure IA for all Air Force procured Information Systems, and Guest systems operating on or accessed from the AF-GIG. The central component used to satisfy policy requirements of DIACAP is the completion of IT Lean and the Security, Interoperability, Supportability, Sustainability, and Usability (SISSU) checklist in the Enterprise Information Technology Data Repository (EITDR). This dynamic application provides an automated certification and accreditation workflow capability. IA will be implemented with IA controls as defined by DoDI 8500.2, *Information Assurance (IA) Implementation* and the DIACAP Knowledge Service, as well as specific IA controls required by the Air Force. Air Force specific IA controls will be limited to those that only affect Air Force ISs and will be posted to the DIACAP Knowledge Service (**https://diacap.iaportal.navy.mil**). Air Force IA controls must be applied to Air Force ISs; Guest ISs are not required to implement Air Force component IA controls.

1.4. Transition from DITSCAP to DIACAP. All ISs are to convert from Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) to DIACAP. In addition to the information below, the *IT Lean Re-engineering Guidebook* provides additional information for systems in various activities of C&A transition. The guidebook is available on the Air Force IA Community of Practice (CoP).

1.4.1. Follow the DIACAP Transition Timeline and Instructions outlined in the DIACAP policy.

1.4.2. PM/SM (or Information System Owner (ISO) if the IS does not have a PM/SM) shall submit a copy of the IS's strategy and schedule to transition to DIACAP as stated in Enclosure 5 of the DIACAP policy. This document will be uploaded in EITDR as an artifact to the system record. If IA Controls are found to be non-compliant, a POA&M is required to be uploaded in EITDR immediately.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Senior Information Assurance Officer (SIAO). AF-CIO has appointed the Deputy Director, Warfighter Systems Integration and Deployment (SAF/XCD-2) as the Air Force SIAO, to direct and coordinate the Air Force IA Program consistent with the strategy and direction of the DoD IA Program. *NOTE:* The term "Senior Information Assurance Officer" is synonymous with the term "Senior Agency Information Security Officer" as defined in FISMA. The SIAO shall:

2.1.1. Establish and enforce the C&A process, roles and responsibilities, and review and approval thresholds and milestones within the Air Force IA Program.

2.1.2. Complete training and maintain appropriate cybersecurity certifications in accordance with (IAW) AFMAN 33-285, *Information Assurance Workforce Improvement Training*.

2.1.3. May delegate Certification Authority for AF SAP/SAR and AF Space systems to respective Lead DAAs (see para 2.3).

2.1.4. Appoints a primary and alternate representatives to serve on the DIACAP Technical Advisory Group (TAG). These representatives will also co-chair the AFCAP TAG.

2.1.5. Approves licensing of Agents to the Certifying Authority (ACA) thru the use of an ACA licensing guide located on the IA CoP.

2.1.6. Ensures the IT Lean Re-engineering Guidebook is coordinated with SAF/AQ prior to release of new versions.

2.1.7. Oversees cybersecurity awareness and education, training (role-based), and professional development programs and ensures cyberworkforce development program aligns with specific requirements outlined in functional guidelines.

2.1.8. In coordination with the SAF/CIO A6 and AF Authorizing Official (AO)(formally DAA), ensures information security risk posture and risk tolerance decisions for AF IS meet mission and business needs while also minimize the operations and maintenance burden on the organization.

2.1.9. Ensures that IS guidelines are incorporated into IT acquisition, implementation, and operations and maintenance functions.

2.2. Deputy Chief of Staff, Intelligence, Surveillance and Reconnaissance (AF/A2). IAW DoDD 8520.1, AF/A2 is the AF Lead for IA of National and AF Sensitive Compartmented Information (SCI) systems (see DoDD 8520.1, *Protection of Sensitive Compartmented Information (SCI),* and AFPD 14-3. *Control, Protection, and Dissemination of Intelligence Information*) and all ISs within AF SCI facilities and is responsible for protection of confidentiality, integrity, and availability of all SCI systems. AF/A2 or other authorized AF entity (e.g. AF Service Cryptological Element) will ensure these requirements are fulfilled in accordance with national and DoD directives and policies. AF/A2 will be the DAA for AF SCI systems and for Guest SCI systems when authorized by National Authorizing Officials. .

2.2.1. The AF appointed authorized entity for national intelligence systems in addition, shall, as requested by SAF/AA, provide SAF/AA with guidance concerning security requirements and implementation of ISs in SCI facilities to include SAP/SAR programs.

2.3. Lead Designated Accrediting Authority (Lead DAA). The Secretary of the Air Force (SAF) appointed AFNETOPS/CC as the AF-DAA, who is the Lead DAA for all Air Force ISs, excluding multi-component space ISs and SAP/SAR ISs. Other Lead DAAs are defined in AFPD 33-2. Lead DAAs shall:

2.3.1. Complete training and maintain appropriate IA certification, if applicable, IAW AFMAN 33-285.

2.3.2. Be able to appoint System DAAs and must hold them accountable for decisions made regarding the security of their IS. Appointments will be documented in writing and a copy will be maintained as an artifact in each accreditation package for IS System DAAs are appointed for. System DAAs must meet the General Officer (civilian equivalent) requirement in AFPD 33-2. Digital signatures are authorized for the appointment letters.

2.3.2.1. Review written requests for appointment of DAA responsibilities. Digital signatures are authorized for the request letters. A DAA appointment request letter template resides within the IA Community of Practice (**https://afkm.wpafb.af.mil/IA**).

2.3.2.2. Ensure System DAAs are identified for only ISs under their purview and that System DAAs have the ability to influence the application of resources to achieve acceptable security.

2.3.3. SAP/SAR & Space Lead DAAs will provide recommendations to the SIAO for delegation of Certifying Authority for systems under their purview.

2.3.3.1. IAW national ISR authorizing official policy, AF entities will be appointed to perform CA responsibilities for all Air Force national intelligence systems (see para 2.2).

2.3.4. On behalf of SAF and consistent with DoD Principal Accrediting Authority (PAA) guidelines and authorities, may appoint System DAAs for Air Force ISs.

2.4. System Designated Accrediting Authority (DAA). The System DAA shall:

2.4.1. Have a level of authority commensurate with accepting, in writing, the risk of operating all ISs under the System DAA's jurisdiction. Must be resourced with individuals knowledgeable in all areas of security to support the System DAA so that technically correct assessments of the security characteristics are made for IS.

2.4.2. Perform functions outlined in DIACAP, as well as the following guidelines: DoDD 8500.01E, DoDI 8500.2; AFPD 33-2; and CJCSM 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)*, 8 March 2006 (Appendix A, Enclosure A).

2.4.3. Complete training and maintain appropriate IA certification IAW DoD 8570.01-M, chapter 5 and CNSSI 4012. Proof of training (e.g. certificate) will be included as an artifact to the IS's C&A package.

2.4.4. Not further delegate accreditation authority. However, System DAAs may designate others to support the accreditation process (e.g. DAA Representative).

2.4.4.1. Appoint DAA Representatives in writing. Digital signatures are authorized for appointment letters, which will be an artifact in the accreditation package.

2.4.4.2. Provide written expectations and specific responsibilities to the DAA Representative upon appointment.

2.4.5. System DAA may delegate to installation commanders or higher the authority to approve IS access (including stored electronic data or communications) for systems under the commander's control in order to support authorized investigative activity conducted by Air Force Office of Special Investigations (AFOSI) or other Law Enforcement personnel.

2.5. DAA Representative. If appointed, DAA Representatives shall:

2.5.1. Perform responsibilities as outlined by the System DAA.

2.5.2. Perform all responsibilities outlined by the DAA except formally accept risk for an IS (i.e. cannot sign the accreditation letter).

2.5.3. Make accreditation recommendations to the System DAA based on input and validation of IA controls from the CAR and/or ACA.

2.5.4. Complete AO(formally DAA) training and maintain appropriate cybersecurity certification IAW AFMAN 33-285 and CNSSI 4012. Proof of training (e.g. certificate) will be included as an artifact to the IS's C&A package.

2.6. Information System Owner. Must be a DoD official (O-6 or civilian equivalent), be a United States citizen, and have a level of authority commensurate with operating the IS on behalf of the Air Force so as to manage the mission risk. The ISO shall:

2.6.1. Be appointed by HAF 2 letter or MAJCOM/CV based on the functional mission area of the system. A copy of the appointment letter must be maintained with the accreditation package.

2.6.1.1. MAJCOM/CV may delegate the authority to appoint the ISO to the MAJCOM functional 2 Letter. HAF 2-letter may delegate the authority to appoint the ISO to the HAF 3-letter.

2.6.1.2. Existing ISOs (i.e. former System DAAs) continue to function as such until a new appointment is done for that system.

2.6.2. Perform all roles and responsibilities of a DAA, with the exception of accepting risk for a system, which can only be done by the DAA in the form of an accreditation decision.

2.6.2.1. Ensure the system is deployed and operated according to the agreed-upon security requirements.

2.6.2.2. In line with this, endorse the POA&M.

2.6.3. Ensure ISs are resourced with individuals knowledgeable in all areas of security to support security engineering and security technical assessments of the IS for the CAs certification determination, AO's (formally DAA) accreditation decision, and other security related assessments (e.g., Financial Improvement and Audit Readiness (FIAR) IT testing, Inspector General audits).

2.6.4. May act as a Reviewer in the IT Lean process. At a minimum will have visibility to the system's C&A progress in EITDR and perform a review prior to allowing the system to move into the next IT Lean Phase.

2.6.5. AFMAN 33-285 instead of DoD 8570.01-M

2.6.6. Program Managers ensure, with assistance from Functional SMEs, that system processes and security controls have been implemented in accordance with specific requirements outlined with in functional guidelines.

2.7. Program Manager. In addition to executing duties cited in other policies, Program Managers shall:

2.7.1. When necessary to complete validation procedures for the program, will plan and fund for an independent Agent of the Certifying Authority (ACA) for each IS to accomplish all validation procedures spelled out in DIACAP Knowledge Service.

2.7.2. Ensure POA&M development, tracking, and resolution as well as implement the corrective actions identified in the POA&M.

2.7.3. Ensure IS details are provided in EITDR and the IT Lean Process.

2.7.4. Enforce DAA accreditation decisions.

2.7.5. Ensure annual security reviews are conducted.

2.8. User Representative (UR). In addition to executing duties cited in other policies, User Representatives shall:

2.8.1. 2.8.1. Complete training and maintain appropriate IA certification, if applicable, IAW AFMAN 33-285.

2.8.2. Represent the user community for a particular system for DIACAP purposes

2.9. Certifying Authority (CA). The Air Force SIAO has delegated the role of CA, for all AF ISs, to AFCA/EV. The CA shall:

2.9.1. 2.9.1. Complete training and maintain appropriate IA certification IAW AFMAN 33-285 and CNSSI 4015.

2.9.2. Perform security validations, conduct a risk analysis, and provide connection recommendations for SAP/SAR, Space, and Guest systems seeking connection to the AF-GIG, using the IT Lean process.

2.9.2.1. Provide final certification recommendation to support System DAA accreditation decisions and AF-DAA connection approval decisions for AF IS using the IT Lean process.

2.9.3. Appoint CARs at the MAJCOM or Functional level as requested by the MAJCOM or Functional.

2.10. Certifying Authority Representative (CAR).

2.10.1. Complete training and maintain appropriate IA certification IAW AFMAN 33-285 and CNSSI 4015.

2.10.2. Serve as an active member of the DIACAP Team from its inception, to assist with planning of IA requirements. These personnel ensure that the implementation and validation procedures are performed as identified in the DIACAP, on behalf of the CA, if these activities are not contracted to an ACA (see 2.11).

2.10.3. Continuously assess and guide the quality and completeness of DIACAP activities, tasks, and the resulting artifacts.

2.10.4. Be directly responsible to the CA, and ultimately the DAA.

2.10.5. Work with the PM and DIACAP team to provide answers and artifacts to SISSU questions which consider the overall reliability and viability of the DoD IS.

2.11. Agent of the Certifying Authority (ACA). The ACA is a licensed organization which may be contracted by the PM to assist in certification activities and shall:

2.11.1. Report directly to the Air Force Certifying Authority (AFCA/EV) for guidance related to validation activities and procedures.

2.11.2. Request licensing approval from the AF SIAO and maintain license IAW with the ACA licensing guide.

2.11.3. Respond to PM's and System DAA's (or ISO) requests for information regarding their respective systems.

2.11.4. Perform comprehensive evaluation of the technical and non-technical security features (IA Controls) of an IT system, determine the degree to which the IS meets its specified security requirements, and provide mitigation recommendations,.

2.11.5. Perform validation procedures of each applicable IA Control as identified in the DIACAP Knowledge Service.

2.11.6. Follow the requirements, standards, and processes set by the SIAO and CA in the ACA Licensing Guide, located in the IA CoP.

2.11.7. Meet the intent of DIACAP's independence between the PM/SM and the individuals performing security testing. Note: The ACA must not be part of the development team or program office. The PM/SM/ISO shall only provide funding for organizations or contractors to perform ACA responsibilities.

2.11.8. Complete training and maintain appropriate IA certification IAW AFMAN 33-285 and CNSSI 4015.

2.12. DIACAP TAG. The DIACAP TAG provides action officer support to the DSAWG in regards to DIACAP. Specifically, the DIACAP TAG implements deliberate methods to incorporate validation and certification needs and lessons learned in the DIACAP Knowledge Service.

2.13. AFCAP TAG. The AFCAP TAG shall:

2.13.1. Be chaired by DIACAP TAG representatives (see paragraph 2.1.4.).

2.13.2. Include membership from MAJCOM and Secretariat/Air Staff functional communities (e.g. USAF/A1, SAF/FM, etc.); one voting member (and sufficient alternates as

required) per MAJCOM and Secretariat/Air Staff functional communities. Members should have a broad understanding of DIACAP, AFCAP, and IA Controls.

2.13.3. Recommend proposed C&A process changes to the DIACAP TAG.

2.13.4. Provide configuration control for AFCAP related services (e.g. IT Lean baseline change requests).

2.13.5. Examine C&A related issues that are common across the Global Information Grid entities and recommend changes to the baseline IA Controls.

2.13.6. Review proposed changes to Air Force IA Control sets (located in the DIACAP Knowledge Service) for compatibility with the baseline IA Controls and with other established IA Control sets.

2.13.7. Advise the AFNETOPS Architecture Integrated Product Team or other IA advisory forums as identified by the Air Force SIAO to determine C&A priorities and resolve cross-cutting issues.

2.14. Information System Security Managers (ISSM)and Information Assurance Officers (IAO). The ISSM has primary responsibility for maintaining situational awareness and initiating actions to improve or restore IA posture as well as conducting annual security reviews of all IA controls and a test of selected IA controls. In addition to the responsibilities listed in RMF, ISSMs and IAOs assigned to Air Force ISs will complete and maintain appropriate IA certification IAW AFMAN 33-285.

2.15. Privileged User will ensure functional communities of interest systems, servers, workstations, peripherals, communications devices, and software are on-line and supported, and maintain appropriate IA certification IAW AFMAN 33-285.

2.16. AFCA/EV. AFCA/EV personnel will perform C&A post-assessment evaluations to assist in identifying network vulnerabilities, providing AF-DAA visibility to network security operations and capabilities, as well as assisting System DAAs with operational security reviews.

Chapter 3

POLICY

3.1. AFCAP.

3.1.1. Completion of the IT Lean process provides for the following possible accreditation decisions by the system DAA:

3.1.1.1. Authorization to Operate (ATO). Authorization granted by a DAA for a DoD IS to process, store, or transmit information. An ATO indicates a DoD IS has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the DAA. ATOs may be issued for up to 3 years. (see Table 3.1. for a correlation of IT Lean and DIACAP processes)

3.1.1.2. Interim Authorization to Operate (IATO). An IATO accreditation decision is intended to manage IA security weaknesses. It is not intended to be a device for signaling an evolutionary acquisition. If IA/security is adequate for the intended processing time, the version of an DoD information system acquired in one of a planned series of acquisition increments or development spirals may (and should) be granted ATO, even if additional or enhanced IA capabilities and services are planned for future increments or spirals. The ATO accreditation decision should not be reserved for DoD information systems for which no change is planned or foreseen. Such thinking engenders an abuse of the IATO accreditation status and an inaccurate portrayal of the DoD information system's IA posture. SAF/XC, as the Air Force Chief Information Officer (AF-CIO), is the only Air Force member that may authorize an Air Force IS to operate (receive an IATO) with "CAT I" weaknesses, as described in DIACAP. Delegation below the AF-CIO is not authorized. Likewise, ISs with CAT I weaknesses, which are accredited by other DoD Components, wishing to connect to the AF-GIG require their component CIO approval, and joint systems require DoD CIO approval.

3.1.1.2.1. Information Systems with unmitigated CAT I vulnerabilities must submit their DIACAP packages to the AF-CIO prior to making an accreditation decision.

3.1.1.2.1.1. After validation of the Build & Test phase in IT Lean the CA will inform the ISO (who acts as the affected military commander as described in DIACAP) to justify the critical nature of the system to military operations and the necessity to allow operation of the system to prevent mission impact.

3.1.1.2.1.2. The ISO will send justification to the AF-DAA Rep, who will then submit the DIACAP Executive package to the AF-CIO with the certification determination and the ISO's request for an IATO for 180 days. That time will be used to mitigate or correct the identified weakness.

3.1.1.2.1.3. The AF-CIO will provide an accreditation decision (IATO or DATO) and return the Accreditation decision to the AF-DAA Rep, who will then upload the decision outcome in to EITDR for continued staffing of the Authorization to Connect (ATC) package.

3.1.1.2.1.4. A copy of the AF-CIO authorized IATO will then be forwarded to the DoD Senior IA Officer (SIAO) and the System DAA.

3.1.1.3. Interim Authorization to Test (IATT). The IATT accreditation decision is a special case for authorizing testing in an operational information environment or with live data for a specified time period. An IATT may not be used to avoid ATO or IATO validation activity and certification determination requirements for authorizing a system to operate. If required and requested, an IATT decision will be provided during the Build & Test phase in IT Lean.

3.1.1.3.1. The term "operational information environment" may be defined as a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. It encompasses physical areas and factors (of the air, land, maritime, and space domains) and the information environment. Included within these are the adversary, friendly, and neutral systems that are relevant to a specific joint operation (Joint Publication 3-0).

3.1.1.4. Denial of Authorization to Operate (DATO). A DAA decision that a DoD IS cannot operate because of an inadequate IA design, failure to adequately implement assigned IA controls, or other lack of adequate security. If the system is already operational, the operation of the system is halted.

3.1.2. A connection approval is the formal approval for an IS to connect to the AF-GIG and the acceptance of risk associated with the IS connection by the AF-GIG Designated Accrediting Authority (AF-DAA) or delegated individual. The AF-GIG connection approval authority shall be delegated only to a qualified government official (see AFPD 33-2) with a rank/grade of O-6 (or civilian equivalent) or higher as follows:

3.1.2.1. Mission Assurance Category (MAC I) systems (see DoDI 8500.2 for guidance). Air Force Network Operations (AFNETOPS)/CC or AFNETOPS/CV has connection approval authority.

3.1.2.2. MAC II systems. AFNETOPS/CC delegates connection approval authority to AFCA/CC or CV.

3.1.2.3. MAC III systems. AFNETOPS/CC delegates connection approval authority to AFCA/EV or EV Deputy.

3.1.2.4. In addition, AFNETOPS/CC may appoint additional connection approval authorities as needed, following the same guidelines as listed in par. 3.1.2.

3.1.2.5. A connection approval decision is acquired by completing the Security discipline of the IT Lean process. AFCA/EV performs an IA review, validates the implementation of the IA controls, and provides comments to AFCA/CC, as the AF-DAA Representative, who in turn provides the approval recommendation to AF-DAA. The AF-DAA will then issue a decision for an ATC. By awarding an ATC, the AF-DAA ensures the IS is certified and accredited (has an approved accreditation decision prior to the ATC decision) and is in compliance with the assigned IA controls to perform mission related activities. More information on the IT Lean process can be found in the *IT Lean Re-engineering Guidebook.*

3.1.2.5.1. Connection approval decisions are limited to:

3.1.2.5.1.1. Authorization to Connect (ATC) to the AFIN/DODIN.

3.1.2.5.1.1.1. An ATC is granted to allow a system to connect to the AFIN. For enclaves requiring a circuit connection from DISA, ISSMs must follow the DISN Connection Process Guide, located at **http://www.disa.mil/Services/Network-Services/Enterprise-Connections/Connection-Process-Guide**, to ensure all required artifacts are provided on initial submission.

3.1.2.5.1.1.2. Systems authorized through the AF Enterprise AO will receive an ATC as the system is reviewed for its authorization.

3.1.2.5.1.1.3. Systems that are authorized by another AO are required, at a minimum, to provide a topology and valid authorization(s) for the system that is being connected. In addition, the following RMF artifacts, or their equivalent, are required: Sponsor memo (for guest systems), scorecard, SIP, PPS, hardware/software list, risk assessment report, and POA&M.

3.1.2.5.1.1.4. Both systems/enclaves involved in the ATC must have a current authorization. The ATC's expiration date will be the earlier of the two authorization package dates (e.g., whichever one expires first).

3.1.2.5.1.1.5. Guest system sponsors or PMs are required to initiate the ATC request in eMASS.

3.1.2.5.1.2. Denial of Authorization to Connect (DATC). AF-DAA determination that an IS cannot connect to the AF-GIG because of an inadequate IA design, failure to adequately implement assigned IA Controls, or other lack of adequate security. If the IS is already connected, the connection of the IS must be terminated. All denial decisions must be signed by the AF-DAA, not delegated to AFCA as for certain approval decisions.

3.1.2.5.2. AF sponsor of Guest ISs is required to enter minimal system information into EITDR and upload Executive DIACAP package or equivalent information to obtain connection approval to the AF-GIG; the IS will be tracked by its DITPR number.

3.1.2.5.2.1. ISs accredited under the authority of the Director of National Intelligence (DNI) use the DNI C&A number as applicable for entry into EITDR and will follow guidance set by DNI for registration. These systems will follow the Guest ISs process as applicable for ATC approval.

3.1.3. Systems for which AFNETOPS/CC is the DAA will have an ISO appointed who will have direct oversight and management (as related to Information Assurance) of the system and will perform all responsibilities outlined in this policy and AFPD 33-2.

3.1.4. POA&M. A POA&M, also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in IT programs and systems. For further POA&M information, refer to the AF POA&M Guide located on the IA CoP.

3.1.4.1. SAF/XCPPI will monitor and track the overall execution of system level IT Security POA&Ms (on behalf of the AF CIO and SIAO) until identified security weaknesses have been closed and the C&A documentation appropriately adjusted.

3.1.4.2. The PM is responsible for implementing the corrective actions identified in the IT Security POA&M and, with the support and assistance of the IAM, provides visibility and status to the ISO, DAA, and SAF/XCPPI.

3.1.5. AF Enterprise AO Authorization timelines.

3.1.5.1. Packages with a licensed Agent of the Security Control Assessor (ASCA) review/recommendation must be uploaded in eMASS at least 30 days prior to mission need date and/or expiration dates of previously provided approvals and pushed to Step 5 (CA Representative review) in eMASS to begin the review.

3.1.5.2. Packages without an (ASCA) review/recommendation must be uploaded in eMASS at least 60 days prior to mission need date and/or expiration dates of previously provided approvals and pushed to Step 5 (CA Representative review) in eMASS to begin the review.

3.1.5.3. The RMF Comprehensive Package must include the System Implementation Plan (SIP), RMF Implementation Plan (DIP), RMF Scorecard, IT Security Plan of Action & Milestones (POA&M), network topology and supporting documentation to include artifacts associated with the implementation of cybersecurity controls. Packages that do not include the required documentation will be given a maximum of five business days to provide the necessary artifacts.

3.1.5.4. Authorization packages that have a residual risk level of CAT I (High or Very High), will require additional time to process the package IAW paragraph 3.1.1.2.1.

3.1.5.5. If the above timelines are not met, the circuit will be at risk for disconnection as directed by US CYBER COMMAND.

Table 3.1. DIACAP Activities Mapped to IT Lean Phases.

DIACAP Activity 1 *Initiate and Plan IA C&A*	*IT Lean Phase 1* *Define Need*
Register System with DoD Component IA Program	Register System with DoD Component IA Program
Assign IA Controls	Assign IA Controls
Assemble DIACAP Team	Assemble DIACAP Team
Initiate DIACAP Implementation Plan (DIP)	Initiate DIP
	Security Validators ensure appropriate IA Controls are assigned based upon assigned MAC and Confidentiality Level (CL)
DIACAP Activity 2 *Implement and Validate Assigned IA Controls*	*IT Lean Phase 2* *Design & Review*
Execute DIP	Populate DIP
Conduct Validation Activities	Security Validators review DIP to ensure plan is IAW DoD and AF security policies
Prepare POA&M	*IT Lean Phase 3* *Build & Test*
Compile Validation Results in DIACAP Scorecard	Execute DIP
	Conduct DIACAP Validation Activities
DIACAP Activity 3 *Make Certification Determination and Accreditation Decision*	Compile Validation Results in DIACAP Scorecard
Certification Determination	Prepare POA&M
Issue Accreditation Decision	Certification Determination
	Issue Accreditation Decision
	Security Validators verify validation procedure results are IAW requirements
DIACAP Activity 4 *Maintain Authorization to Operate and Conduct Reviews*	*IT Lean Phase 4* *Release & Support*
Maintain Situational Awareness	Maintain Situational Awareness
Maintain IA Posture	Maintain IA Posture
Conduct Reviews (Review of IA Controls must occur at least annually)	Conduct Reviews (Review of IA Controls must occur at least annually)
Initiate Re-accreditation	Initiate Re-accreditation
DIACAP Activity 5 - Decommission	Retire System
Retire System	Information Assurance Manager (IAM) performs annual assessment and Security Validators perform random assessments to ensure continuing compliance with DIP

3.2. Registration.

3.2.1. All systems on which AF dollars are spent must be registered in EITDR, the official Air Force registration vehicle for ISs, with the exception of those identified by other policy (e.g. SPACE, Special Access Programs/Special Access Required, Joint, etc), to be registered in another registration vehicle. EITDR will systematically assign a temporary registration number for each IS until the next scheduled replication with DoD Information Technology Portfolio Repository (DITPR). A DITPR number will then be systematically assigned and included in EITDR as the permanent "official" information technology (IT) registration number. See *IT Lean Re-engineering Guidebook* for procedures on how to use EITDR.

3.3. IT Lean. The IT Lean process is a tailored version of the DoD 5000 series acquisition process that must be applied to small IT programs when appropriate and approved by the Milestone Decision Authority. When used in conjunction with the IT Lean process, this tailored process replaces the Certificate of Networthiness and Certificate to Operate processes through the use of the ATC process.

3.3.1. The IT Lean process applies to systems in acquisition or sustainment including upgrades or modernizations. A modified IT Lean/SISSU process will also be used for commercial off the shelf (COTS) and government off the shelf (GOTS) products being integrated into the AF-GIG. The requirements of DOD 5000 series; Chairman, Joint Chief of Staff Instruction 3170.01F, *Joint Capabilities Integration and Development System*, 1 May 2007; Chairman, Joint Chiefs of Staff Manual 3170.01C, *Operation of the Joint Capabilities Integration and Development System*, 1 May 2007; and AFI 10-601, *Capabilities Based Requirements Development*, 31 July 2006 still apply. The program scope for the IT Lean process is limited to programs that meet all of the following criteria:

3.3.1.1. Must be an IS as defined in DoDI 5000.2, *Operation of the Defense Acquisition System*.

3.3.1.2. Designated acquisition category (ACAT) III (as defined in DoDI 5000.2) or Non-ACAT with a $15M or below – in development or enhancement costs; and must have a Joint Potential Designator (JPD) of "Independent" (programs with no JPD are assumed to be "independent").

3.3.1.3. Approval to enter the IT Lean process from the appropriate acquisition authority (See references listed for additional guidance).

3.3.2. The IT Lean process provides a standardized and streamlined approach to develop and field SISSU compliant IT capabilities. The process has four distinct phases: Define Need, Design, Build and Test, and Release and Support. The process has five milestone reviews: Define Need Review (DNR), Design Review (DR), Test Readiness Review (TRR) I and II, and Field Readiness Review (FRR). IT Lean is consistent with the DIACAP 5-activity approach.

3.3.3. Air Force IS which have not been designated as SPACE or Special-Access Program/Special Access Required (SAP/SAR) systems will complete the IT Lean process to obtain an ATO. In addition, all ISs connecting to the AF-GIG must obtain an ATC using IT Lean (see Table 3.2.).

3.3.3.1. Additionally, use of PPS required for the ISs to operate through a firewall on the AF-GIG, will be registered by the Security Validators at the completion of Phase 2 of the IT Lean process.

3.3.3.1.1. PPS for Guest systems will be provided to the AFNOC NOG for AF PPS registration.

3.3.3.2. Systems which process classified information may follow the IT Lean process in EITDR if the actual artifacts and documentation do not include classified information. Users must work directly with AFCA/EVSS to address classified components of a C&A package.

Table 3.2. IT Lean Process.

Connection Status	New or non-accredited Air Force IS	Previously accredited Air Force IS with modifications or re-accreditation requirements	Guest IS seeking connection to AF-GIG (ATC)
Networked	The PM/SM/ISO is responsible for entering information in EITDR for the purpose of completing IT registration, ATO and ATC processes. The PM/SM/ISO directs and manages completion of IT Lean and SISSU.	The PM/SM/ISO will enter information in EITDR, host an initial stakeholder meeting, and initial security review to determine if a new version is to be created. If changes will not affect the security posture of the IS, the PM/SM/ISO will annotate the outcome of the meeting and make necessary edits to the C&A package. If security changes will occur, a new IT Lean version will be created within EITDR and will re-enter the IT Lean process for an ATO and ATC.	Guest ISs completing C&A outside of IT Lean must submit a request for ATC to SAF/XC. The SIAO will then appoint a functional sponsor for the system requesting the ATC. The AF sponsor will then enters the system into EITDR and act as a liaison with the external customer to complete IT Lean process for Guest systems. AF Sponsor uploads the DIACAP executive package (or other authorized format for the C&A package) and MOU/SLA if applicable The AF-CA then reviews the package and issues and a connection decision (AFCA/EV for MAC III, AFCA/CC for MAC II) or forwards the package and recommendation to the AF-DAA for connection decisions regarding MAC I

Connection Status	New or non-accredited Air Force IS	Previously accredited Air Force IS with modifications or re-accreditation requirements	Guest IS seeking connection to AF-GIG (ATC)
			systems. AF Sponsor will provide the requestor with the connection decision (ATC/DATC) documentation. The decision outcome will then be made available to the field.
Stand-Alone	The PM/SM/ISO will enter information in EITDR for the purpose of completing IT registration and the ATO process only. A DATC will be automatically assigned.	The PM/SM/ISO will enter information in EITDR to host an initial stakeholders meeting and initial security review to determine what path should be taken. If changes will not affect the security posture of the IS, the PM/SM/ISO will annotate the outcome of the meeting and make necessary edits to the C&A package. If security changes will take place, a new IT Lean version will be created in EITDR and re-enter the IT Lean process for an ATO.	Not Applicable

3.4. Software (COTS & GOTS).

3.4.1. Software is computer code that executes on behalf of the operating system, using the services of the computer's operating system and other supporting software to perform a specific function directly for the user or another software program.

3.4.1.1. Government off the shelf software (GOTS) is developed by the technical staff of the government agency for which it is created. It is sometimes developed by an external entity, but with funding and specification from the agency.

3.4.1.2. Commercial off the shelf software (COTS) is software that is ready-made and available for sale, lease, or license to the general public. To include software developed, tested, and sold by commercial companies to the general public. Examples include word processors, databases, application generation, drawing, compiler, graphics, communications, and training software.

3.4.1.3. Specific web services as described in DODI 8500.10 could be included under the COTS process.

3.4.1.3.1. Web Services. Self-describing, self-contained, modular units of software application logic that provide defined business functionality. Web services are consumable software services that typically include some combination of business logic and data. Web services can be aggregated to establish a larger workflow or business transaction. Inherently, the architectural components of Web services support messaging, service descriptions, registries, and loosely coupled interoperability.

3.4.1.3.2. Web service may also be required to meet minimum standards imposed by the host information system. For example, web services installed on the AF Portal have specific security requirements that must be met prior to implementation.

3.4.2. All software planned for use or in use on the AF-GIG must be certified for placement on the Air Force Evaluated/Approved Product List. This also includes hardware devices that contain embedded software. For a detailed step by step process see the IT Lean Re-engineering and IT Lean Process Guide Book located on the AF IA COP. If the software is part of a system then it gets C&A through the normal IT Lean process, only software not part of a system goes through the COTS process.

3.4.2.1. Applications are considered software programs that perform a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs.

3.4.2.2. Information Systems are a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Systems include AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

3.4.2.3. If it does not fit the definition of an Information System or is excluded by another rule, it is by default an application. It cannot be an application if it meets the requirements of an Information System.

3.4.3. All software submissions must flow through the enclave Configuration Control Board (CCB) in which it is meant to be implemented to ensure the CCB has a current and comprehensive baseline inventory of all software and hardware, establishing a single focal point for submissions into the process.

3.4.3.1. Potential Users/Sponsors (heretofore called Sponsors) of product must fill out the Software Request Worksheet and submit it to their requirements review office. The worksheet can be found on the IA Community of Practice website.

3.4.3.2. The CCB determines if this is a suitable requirement and forwards approved requests to AFCA/EVSN for processing. A suitable requirement includes; a substantiated mission need, available funding, and core functionality that is not already available in currently certified products as well as the Air Force Standard Desktop (SDC).

3.4.3.3. The CCB should determine if the requested software is already on the AF E/APL (located on the IA CoP). If the software is already on the AF E/APL, then the CCB can approve the request without contacting AFCA/EVSN and add the software to the software/hardware baseline. The sponsor will then be allowed to implement the new software.

3.4.4. When an approved request is received by AFCA/EVSN they will review the Software Request Worksheet and determine the testing and documentation required for certification. AFCA may request the sponsor to provide one copy of the software for testing purposes (all products will be returned to the sponsor after completion of testing). AFCA/EVSN will also determine if the product is a candidate for a certification letter. If the product is a desktop product that will reside within the SDC and is not part of a larger system, then the product can be issued a certification letter.

3.4.4.1. If a certification letter is issued then the CCB adds the product to the software/hardware baseline and allow the sponsor to implement the software. Once the certification letter is issued the product will be placed on the AF E/APL.

3.4.4.2. If the software is not a desktop product, AFCA/EVSN can only issue a certification letter. The certification letter states that the software meets DoD IA controls and is a low risk to the network. The sponsor will then be required to include the software as part of, or as, an IS and complete the IT Lean process in order to implement the software on the network.

3.4.4.3. If the product testing results do not meet the Air Force security standards the product sponsor will be notified by AFCA/EVSN that the product is not approved for use on the AF-GIG at this time. Note: Even products that are disapproved will be posted to the AF-E/APL (as Disapproved), this will preclude resubmission of previously disapproved products.

3.4.4.3.1. If the product under test produces positive results AFCA/EVSN will submit a certification letter recommendation to AFCA/EV (AF Certification Authority (AF-CA). This recommendation (if signed by the AF-CA) will be used to authorize posting of new products on the AF-E/APL and publication of the certification letter.

3.4.5. Implementing sites must ensure they adhere to specific guidance in the certification letter and associated installation/configuration guides located on the E/APL prior to installing the COTS/GOTS.

3.5. Changes to Systems with an Established ATC. The requirements for systems to maintain their certification and accreditation status after the implementation of a change are listed in the following paragraphs.

3.5.1. The system must have been previously assessed by AFCA/EVSS and granted an Air Force network connection authorization (ATC) in IT Lean.

3.5.2. The system IAM reviews proposed changes and determines if system and network security will be affected by the release of these changes and communicates the results of the IAM review to the CA & System DAA. Continued approval to operate and connect is contingent on the sustainment of an acceptable IA posture.

3.5.2.1. The system IAM provides a written or DoD PKI-certified digitally signed statement to the CA (AFCA/EVSS) and DAA indicating the results of the security review and declaring system and network security have not been affected by the changes. That statement will be uploaded into EITDR as artifacts until EITDR is capable performing digital signature.

3.5.3. Any changes which negatively affect security cannot be considered a minor change and must; therefore be revalidated using the Security Discipline of IT Lean.

3.5.3.1. If the IS is an Air Force system, the IAM must notify the PM who will initiate a new version in IT Lean and complete all phases of the Security Discipline.

3.5.3.2. Sponsors or PMs of Guest systems are required to initiate a new version in IT Lean and submit an updated DIACAP Executive Package for review.

3.5.3.3. If a new version has been entered in EITDR, the PM also must identify if this system is replacing a previous version, and if so, take appropriate actions to decommission the previous version. See *IT Lean Re-engineering Guidebook* for decommissioning procedures.

3.6. Deleted.

3.6.1. Deleted.

3.6.2. Deleted.

3.6.3. Deleted.

3.6.4. Deleted.

3.6.5. Deleted.

3.6.5.1. Deleted.

3.6.5.2. Deleted.

3.6.5.3. Deleted.

3.6.5.3.1. Deleted.

3.6.5.3.2. Deleted.

3.6.5.3.3. Deleted.

3.6.5.3.4. Deleted.

3.6.6. Deleted.

3.6.6.1. Deleted.

3.6.6.2. Deleted.

3.6.6.2.1. Deleted.

3.6.6.2.2. Deleted.

3.6.6.2.3. Deleted.

3.6.6.2.4. Deleted.

3.6.6.2.5. Deleted.

3.6.6.2.6. Deleted.

3.6.6.2.7. Deleted.

3.6.6.2.8. Deleted.

3.6.6.2.9. Deleted.

3.6.6.2.10. Deleted.

3.7. Post-Accreditation Reviews & Assessments.

3.7.1. Phase 4 (Release and Support) of IT Lean incorporates annual reviews to ensure the IS continues to operate in the manner in which it was certified and accredited. These reviews are a requirement in FISMA guidelines and are reported annually to DoD and OMB.

3.7.2. IAMs will conduct a review of all applicable IA controls and perform validation procedures on those controls as identified in the annual FISMA reporting requirements

3.7.3. AFCA/EV will conduct random assessments on IA Control compliance to give AFNETOPS operational oversight of the security of the AF-GIG. The assessment will consist of performing validation procedures on a sub-set of the IA Controls. These assessments may then count as annual reviews for the IAM, but it will be up to the IAM to identify, mitigate, and correct findings in the FISMA reporting section of EITDR.

3.8. Circuit-Enclaves.

3.8.1. As defined by DoDI 8500.2, an enclave is a collection of computing environments connected by one or more internal networks under the control of a single approval authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in OMB A-130 (reference (n)). Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers. The most common Air Force circuit-enclaves are base networks; however, systems that use dedicated DISA-provisioned circuits and in doing so form isolated networks, are by definition circuit-enclaves. The latter must still adhere to all DISA Connection Approval Process (CAP) requirements, but are not considered circuit-enclaves for the purposes of this instruction and the processes outlined within.

3.8.1.1. Air Force owned and operated enclaves receive connection to the DISN via DISA provisioned circuits and require a valid accreditation to do so. These enclaves are referred to as circuit-enclaves since each is connected to one or more unique DISA provisioned circuits. Each DISA provisioned circuit is assigned a unique Command Communications Service Designator (CCSD) for identification and tracking purposes. Each CCSD related to a circuit-enclave must be referenced in the appropriate circuit-enclave accreditation package.

3.8.2. All Air Force owned and operated circuit-enclaves must follow the SISSU process using EITDR to receive an accreditation which will be used for the subsequent DISA Approval to Connect process. The base-level PM/SM or IAM is responsible for EITDR registration; for enclaves without a PM/SM, the ISO is responsible for ensuring this registration is completed. The process for EITDR registration and SISSU is outlined in the IT Lean Guidebook.

3.8.3. The Air Force network is accredited using the Combat Information Transport System (CITS) Block 30 gateway construct. There is one accreditation package for each of the 16 NIPRNet and SIPRNet gateways for a total of 32 gateway accreditation packages. Each of these 32 gateway packages is comprised of multiple base-level enclave sub-packages. Any enclave not assigned to a CITS gateway is accredited on a case-by-case basis.

3.8.4. The circuit-enclave accreditation process will utilize IA Control inheritance to complete C&A packages. The primary source for infrastructure IA Control inheritance shall be CITS Lead Command. Circuit-enclave PMs will coordinate with the CITS Lead Command office to obtain inherited IA Control implementation information.

3.8.5. Unique Circuit-Enclave Accreditation Scenarios

3.8.5.1. Exercise circuits

3.8.5.1.1. The requirements for exercise circuits may vary from operational circuits. Refer to the IASE website (**http://iase.disa.mil**) for these requirements.

3.8.5.2. Cross Domain Solutions (CDS)

3.8.5.2.1. Systems that operate cross domain solutions have additional accreditation requirements as outlined in CJCSI 6211.02B, *Defense Information System Network (DISN): Policy, Responsibilities and Processes* (to be superseded by CJCSI 6211.02C). All Air Force requests to operate cross domain solutions must be coordinated through the AFCA Cross Domain Solutions Office (CDSO) located at Scott Air Force Base. The AFCA CDSO may be contacted at DSN 779-6498; Commercial (618) 229-6498 email **afcaea3.cdso@scott.af.mil** . CDS connections have additional requirements. Refer to the IASE website for this process and associated documentation requirements, as well as the CDSO for assistance.

3.8.6. Roles and Responsibilities.

3.8.6.1. DISA.

3.8.6.1.1. The connection approval authority for all DISN/DVS connections. The connection approval process and associated requirements are outlined in CJCSI 6211.02B and the IASE website.

3.8.6.2. CITS Lead Command:

3.8.6.2.1. Responsible for the design and implementation of the Air Force Architecture to include CITS Block 30.

3.8.6.2.2. Maintains and updates the CITS architecture system accreditation package.

3.8.6.2.3. As the provider of numerous IA services via the CITS architecture, CITS Lead Command is responsible for providing and maintaining the answers to all inheritable IA controls for which they provide services. These inherited controls and the associated answers will be maintained in EITDR.

3.8.6.3. AFCA

3.8.6.3.1. Is the SISSU security validator of the circuit-enclave accreditation packages and assumes all associated responsibilities as defined in the IT Lean Reengineering and SISSU Process Guidebook.

3.8.6.3.2. AFCA/EV is the certifying authority for the Gateway accreditation packages.

3.8.6.4. AFNetOps

3.8.6.4.1. AFNetOps/CC will serve as the Designated Accrediting Authority (DAA) for all Air Force circuit-enclaves unless explicitly delegated to an individual meeting the requirements as outlined in AFPD 33-2.

3.8.6.4.2. Maintains the consolidated gateway circuit-enclave accreditation packages in the AFNETOPs portfolio and any portfolio management functions this will require. It will maintain all administrative oversight of these packages including ensuring updates are made to base-enclave packages and routing for validation and DAA signature.

3.8.6.4.3. Serves as the primary Air Force administrative point of contact to DISA Unclassified Connection Approval Office (UCAO) for NIPRNet connection requests and the SIPRNet Connection Approval Office (SCAO) for SIPRNet connection requests. In this capacity AFNetOps will provide Air Force circuit-enclave accreditation status information, provide the necessary accreditation support documentation and field all documentation requests from DISA.

3.8.6.4.4. Stores and maintains any Air Force-level supplemental accreditation documentation. This includes the SIPRNet and NIPRNet Air Force level Consent To Monitor (CTM) as well as standardized topology maps and SIPRNet Connection Questionnaire (SCQ). AFNetOps will ensure these documents are updated by the Enclave ISO prior to submitting for accreditation. For DISA documentation requirements unique to the circuit accreditation process refer to CJCSI 6211.02B and the IASE website.

3.8.6.4.5. Ensures the consolidation of base-level enclave accreditation sub-package POA&Ms into the Gateway-level POA&Ms.

3.8.6.4.6. Tracks the accreditation status of all Air Force circuit-enclaves and ensures a current accreditation is maintained. In doing so, AFNetOps is responsible for ensuring all necessary actions are taken by the responsible parties for maintaining compliance.

3.8.6.4.7. Notifies enclave accreditation sub-package owners of pending accreditation expiration at a minimum of 30, 60, and 90 day intervals.

3.8.6.4.8. Ensures gateway accreditation packages are submitted for re-validation and re-accreditation as a result of any updates to the enclave packages.

3.8.6.5. I-NOSC.

3.8.6.5.1. I-NOSCs must provide an SLA to circuit-enclave PMs outlining any operational network services, related to enterprise IA activities, for which they are responsible.

3.8.6.5.2. The I-NOSCs shall assist AFNetOps in taking necessary action to ensure a current accreditation is maintained by serving as an intermediary between AFNetOps and the circuit-enclave PMs. The I-NOSCs will assist PMs in the development of C&A packages by providing any technical information necessary to accurately answer IA controls for which the I-NOSCs provide operational network services.

3.8.6.6. Enclave Information System Owner (ISO).

3.8.6.6.1. The circuit-enclave Information System Owner (ISO) (as defined in AFPD 33-2) must ensure an IAM is appointed to maintain the IA posture of the circuit-enclave; this individual assumes all responsibilities of the IAM described herein and DODI 8510.01. If no IAM is appointed, the circuit-enclave ISO assumes all IAM responsibilities.

3.8.6.6.2. Enters and completes respective enclave sub-packages within EITDR for the assigned gateway circuit-enclave accreditation package.

3.8.6.6.3. Updates respective circuit-enclave accreditation packages within EITDR to reflect any changes made to their enclaves.

3.8.6.6.4. Alerts AFNetOps of any changes to the topology or software affecting the security posture of the enclave boundaries so that the gateway package can be reaccredited if necessary.

3.8.6.6.5. Updates all supporting documentation required for their circuit-enclave accreditation sub-packages including SCQs and topology maps.

3.8.6.6.6. Enters and updates DISA CAP records within the SNAP database.

3.8.6.7. Other System ISOs/PMs/SMs

3.8.6.7.1. It is the responsibility of an information system owner to notify the enclave ISO of any system changes so the enclave ISO can determine if said changes will impact the enclave and its security posture in any way.

3.9. Exercises.

3.9.1. All exercises performed on the AF-GIG require an IATT from the System DAA, an ATC signed by AFNETOPS/CC, and must follow appropriate policies regarding exercise connections (e.g. CJCSI 6211.02B, CJCSI 6510.01E).

3.9.2. Exercise requests will be coordinated thru AFNETOPS/A3 to determine applicable processes required to obtain the ATC and assign a priority status for security validation.

3.9.3. Expected impacts to systems (which includes enclaves), will be coordinated with ISOs and DAAs thru an SLA/MOA/MOU.

3.9.3.1. Impacts and changes are defined in a Version Description Document (VDD)

3.9.4. Systems which are expected or intended to become operational upon termination of the exercise are required to follow normal system ATO/ATC C&A processes.

3.9.5. POA&Ms are to be provided for systems which have identified vulnerabilities in previous versions or exercises. Classified systems will provide their POA&M s over the SIPRNET since classified information cannot be entered into EITDR.

3.10. Networked Medical Devices. Networked medical devices follow approved C&A policy, including IT Lean. Changes to networked medical devices may not be able to occur in a timely fashion or at all due to regulatory requirements (e.g. maintaining Food and Drug Administration certification) and will be part of the assumed risk for that IS. In some cases, medical equipment may be considered Platform IT and follow IA and C&A policies accordingly.

3.11. Cross Domain Solutions. Systems that operate cross domain solutions have additional accreditation requirements as outlined in CJCSI 6211.02B (to be superseded by CJCSI 6211.02C). All Air Force requests to operate cross domain solutions must be coordinated through the AFCA Cross Domain Solutions Office (CDSO) located at Scott Air Force Base. The AFCA CDSO may be contacted at DSN 779-6498; Commercial (618) 229-6498 email **afcaea3.cdso@scott.af.mil**

3.12. Foreign National Access. Specific requirements for accessing information systems must provided in the DIACAP Implementation Plan (DIP). Procedures for foreign nationals requiring access must also be included in the DIP. See AFSSI 8522, *Access to Information Systems* for guidance.

3.13. Protective Distribution System (PDS). Communication Security (COMSEC) policy calls for a PDS to physically secure unencrypted, classified transmission lines in unsecured areas. This requirement must be built into the solution. See AFI 33-201, Vol 8 *Computer Security: Protected Distribution Systems (PDS)* (will become AFSSI 7703) for further guidance.

3.14. Type Accreditation. DODI 8510.01 defines type accreditation as the official authorization to employ identical copies of a system in specified environments. This form of C&A allows a single DIACAP package (i.e., SIP, DIP, supporting documentation for certification, DIACAP Scorecard, and IT Security POA&M (if required)) to be developed for an archetype (common) version of an IS that is deployed to multiple locations, along with a set of installation and configuration requirements or operational security needs, that will be assumed by the hosting location. Automated Information System (AIS) applications accreditations are type accreditations. Stand-alone IS and demilitarized zone (DMZ) accreditations may also be type accreditations.

3.14.1. Type accredited systems follow the DIACAP process as outlined in DODI 8510.01 and requires an accreditation decision and AF connection approval prior to deployment thru the use of the IT Lean Process.

3.14.2. An approved accreditation and AF connection decision for a type-accredited system is valid for implementation at all AF sites (enclaves). Coordination with the enclave IAM and any updates to all appropriate enclave accreditation documentation is required prior to implementation at any AF site.

3.14.3. A type-accredited system must have centralized program management (PM) oversight to ensure implementation at multiple locations is satisfactorily implemented IAW with the DIACAP Implementation Plan and that implementation plan and any associated configuration guidance is provided to each site implementing the type accredited system.

3.14.3.1. For each IA control expected to be implemented by the local enclave (inherited), the system PM must provide minimum implementation guidelines and requirements expected to be met by the implementing enclave. In other words, the system will identify minimum requirements for all IA controls; regardless if the system implements the IA Control itself, or if it will be inherited by the enclave in which it is being deployed and implemented.

3.14.3.2. To ensure type accredited systems can be implemented at all intended sites (enclaves) using the implementation guidelines provided, the PM should identify site representatives on the stakeholders list and consult them during each phase of IT Lean.

3.14.3.3. All site-specific weaknesses resulting from the implementation of a type-accredited system will be identified in the system POA&M. It is a programmatic (PM) responsibility to ensure those weaknesses are addressed/mitigated or accepted at a program/system level (and not left up to the individual sites/enclaves to address). System versioning cannot be utilized to avoid addressing site-specific weaknesses. All weaknesses (include those that are site-specific) must be adequately addressed per the

requirements outlined in DODI 8510.01 before an ATO can be issued for a type-accredited system and the guidelines regarding the issuance of consecutive IATOs still applies.

3.14.3.4. It is PM responsibility to ensure site coordination prior to system deployment and to ensure the site (enclave) IAM has reviewed the type-accredited system accreditation documentation, assessed the impact the introduction of this system will have on the enclave and, if necessary, updated all applicable enclave-specific accreditation documentation prior to implementation.

3.14.3.5. Each funding source associated with a type accredited system must be accounted for in its associated system resource table maintained in EITDR.

3.14.3.6. In the event that the system-appointed IAM is not implementing the type-accredited system at the local enclave, it is the responsibility of the enclave IAM to ensure the system is implemented in accordance with the implementation guidance provided by the system PM.

3.14.3.6.1. The IAM implementing the type-accredited system must sign a memo attesting to conformance to the system implementation and configuration guidelines and provide said memo to the system PM to file with the C&A documentation. To ensure system accountability and PM oversight, there must be an IAM-signed memo on file with the PM for each implementation of a type-accredited system.

3.14.3.6.2. If at the time of implementation it is determined the type-accredited system cannot be implemented IAW its implementation plan and associated configuration guidance, the system IAM must coordinate with the PM to resolve these issues or update the type-accredited system POA&M to reflect these outstanding non-compliance issues as necessary (see 3.15.3.3).

3.14.3.7. The system IAM ensures annual reviews and FISMA requirements are performed IAW associated policies for every configuration implementation of that type-accredited system. System and Enclave IAMs must will elevate any identified security issues to PM, CA, & DAA.

3.14.3.8. It is the responsibility of the appointed type-accredited system IAM to mitigate and identify IA vulnerabilities, and report and respond to IA violations and incidents IAW DODI 8500.2. This includes ensuring all ongoing security requirements (to include items such as patch management) are met.

3.15. Stand-Alone IS. Stand-Alone systems may be single machines, enclaves, or IS fielded at multiple locations (may be type accredited); which, are not physically connected to any other network. Each configuration of the Stand-Alone IS must have its own IT Lean version approved.

3.16. IT Lean Re-engineering Guidebook. The *IT Lean Re-engineering Guidebook* is the Air Force's resource for implementing and executing C&A in the acquisition process. The *IT Lean Re-engineering Guidebook* supports the policies in this AFI by providing specific procedures and is capable of implementing changes as industry and policy dictate. The IT Lean Re-engineering Guidebook will be coordinated with SAF/AQ prior to new releases to the field.

3.17. ACA Licensing. The number and complexity of ISs in the Air Force make it necessary for the CA to designate qualified entities as ACAs to perform certification actions. The *Agent of the Certifying Authority Licensing Guide* establishes processes for applying for a license to conduct assessments and validations, evaluation of the license request, recommendation for award of a license, and award of an ACA license by the Air Force Chief Information Officer (AF CIO).

3.18. Software Research, Development, Testing, & Evaluation (RDT&E) Enclaves. Enclaves considering themselves Software RDT&E enclaves must review DISA's Enclave STIG to determine the appropriate architecture zone. Enclaves which meet the Zones A&B criteria will complete C&A using the AFCAP. Enclaves meeting Zones C&D criteria as described in the Enclave STIG will only register their enclaves in EITDR and not be required to perform C&A. The Zone C or D enclave IAM must ensure that technical and non-technical controls are employed to isolate these systems from unauthorized access and exploitation IAW the DISA STIG and CJCSI 6510.01.

3.18.1. Zone D: Stand-Alone Test Environment. Zone D systems refer to a single system or collection of systems that have no network connectivity other than to themselves (except in rare cases where there is an ISP connection with ASD and GIG waiver approval). The system or collection of systems must be completely closed and isolated. There are no direct external (DoD, AF or Internet) connections.

3.18.2. Zone C: Closed Network Test Environment. In Zone C, the network may be completely closed and isolated; or connected only to another Zone C testing facility or Zone C subnet. Traffic is isolated and restricted via source and destination IP addresses or host names. There are no direct external (DoD or Internet) connections to these networks. The network connectivity to another Zone C testing facility or subnet may be accomplished via tunneling mechanisms such as VPNs, private circuit (preferred method), TACLANE, MPLS, or other means of complete traffic isolation. At no time will the Zone C system data be commingled with the General Business Enclave LAN or with DoD network traffic.

3.18.3. Zone B: Limited External Network Connected Environment. Zone B systems require external access utilizing a DoD network as the transport mechanism.

3.18.4. Zone A: Full DoD Network Connectivity. Zone A systems require external (live/production) access and may mirror a live, production environment for final stage testing and development.

3.19. Platform IT (PIT), Platform IT Systems (PIT Systems), and Research, Development, Test, & Evaluation (RDT&E) systems.

3.19.1. Cybersecurity risk for PIT, PIT Systems, and RDT&E systems may only be accepted by an AO appointed by SAF/CIO A6. Risk acceptance must be clearly documented by the AO before a system may commence testing or operations in the form of an ATO, ATO with conditions, IATT, or other digitally-signed authorization decision. The AO will provide specific guidance on how the C&A package for a PIT, PIT System, or RDT&E system will be developed and submitted.

3.19.1.1. Normally C&A is not required for Platform IT, however Security requirements must be addressed in system design and operation as prescribed in Acquisiton policies.

3.19.1.2. If the Platform IT has connectivity to an external network then C&A is required as a Platform IT Interconnection

3.19.2. All PIT, PIT System, and RDT&E systems will fall within the authorization boundary of an AO. The authorization boundaries will be specified in the AO appointment letter. In addition, the boundary definitions will be posted to the AFCKS AFCAP site, **https://cs1.eis.af.mil/sites/AFCKS/Compliance/AFCAP/SitePages/Home.aspx**. For questions regarding authorization boundaries, contact the SAF/CIO A6 Cybersecurity Division, **usaf.pentagon.saf-cio-a6.mbx.a3ci-a6ci-cybersecurity@mail.mil.**

3.19.2.1. C&A packages are required for Platform IT Interconnections and should focus on the interconnection(s), not the Platform IT itself. Document any additional measures required of external network to extend IA services or to protect the platform IT from interconnection risk.

3.19.2.2. IA Controls must be selected as applicable and consider the mission assurance category and confidentiality level of both the Platform IT and its interconnecting IT.

3.19.3. For a system to be approved to be PIT, PIT System, or RDT&E, the PM must obtain an approved Determination Letter.

3.19.3.1. PMs will submit a Determination package IAW the respective *Information Assurance Platform IT Guidebook*, **https://cs1.eis.af.mil/sites/AFCKS/Compliance/AFCAP/Shared%20Documents/Guides/IA_PIT_Guidebook_v1.5.pdf**, or the *Air Force Research, Development, Test, and Evaluation (RDT&E) Implementation Guide*, **https://eis.af.mil/cs/rdte/Resources/AF%20RDTE%20Implementation%20Guide%20-%20September%202011.pdf**.

3.19.3.1.1. ICS is a general term that encompasses several types of control systems:

3.19.3.1.1.1. Supervisory Control and Data Acquisition (SCADA), Centralized control of dispersed assets, such as a metropolitan electrical network.

3.19.3.1.1.2. Distributed Control Systems (DCS) - Control production systems within a local area, such as a power plant.

3.19.3.1.1.3. Programmable Logic Controllers (PLC) - Discrete control for specific applications, such as a thermostat.

3.19.3.1.2. Follow the rules for Platform IT and Platform IT Interconnection as applicable

3.19.3.1.3. System Security Plans and IA strategies as defined in Acquisition policies must consider using a cross-walk of the DoD IA Controls and the NIST Security Controls in an effort to meet security requirements.

3.19.3.2. The results of the determination will be returned to the PM and ISSM for the system. 3.19.3.3. The PM will work with the SCA to determine the specific C&A process and applicable security controls for their system.

3.19.3.2.1. Follow the rules for Platform IT and Platform IT Interconnection as applicable. Also C&A is required for the M&S Enclave itself (i.e. the network infrastructure in the M&S Enclave

3.19.3.2.2. Treat training/exercise type M&S Enclaves as "Platform IT" and just focus on the interconnectivity of the Enclaves. The IAM is responsible for the internal Enclave security.

3.19.4. PMs are responsible to identify candidate PIT systems and document PIT determinations in their program's Cybersecurity Strategy.

3.19.5. PIT, PIT System, and RDT&E systems require cybersecurity risks to be identified continually and assessed throughout system design and operation. PMs must establish a cybersecurity risk management program. PMs should use a multi-disciplined Integrated Product Team (IPT) or equivalent science/research team to identify and assess cybersecurity risk. The team should include all necessary stakeholders and will recommend risk management solutions to the PM.

3.19.6. PIT PMs will use the *Information Assurance Platform IT Guidebook* developed by the Platform IT Working Group to assist with the C&A of their systems. The current version of the guidebook can be found on the AFCKS, **https://cs1.eis.af.mil/sites/AFCKS/Compliance/AFCAP/Shared%20Documents**.

3.19.7. RDT&E PMs will use the AF RDT&E SharePoint site, **https://eis.af.mil/cs/rdte**, for specific procedures to assess and authorize their systems.

3.20. Real Time Services.

3.20.1. Real Time Services (RTS) are defined as IP-based network, two-way voice, and/or video capabilities, not wireless, and official conferencing capable. Examples include, but are not limited to: Voice over Internet Protocol (VoIP), Voice over Secure Internet Protocol (VoSIP), Video Teleconferencing over Internet Protocol (VTCoIP), Video Teleconferencing over Secure Internet Protocol (VTCoSIP), and Voice and Video over Internet Protocol (VVoIP). This policy does not cover Internet Protocol Television (IPTV), Land Mobile Radio (LMR), or Radio over Internet Protocol (RoIP).

3.20.2. This applies to all implementations of AF RTS capabilities connecting to AF enclaves configured within the AFIN boundary to include IP VTC capabilities registered within the Defense Information Systems Agency (DISA) Defense Information Systems Network Video Services (DVS).

3.20.3. All AF RTS capabilities supported by AF enclaves must be implemented using components listed on the DISA Approved Products List Integrated Tracking System (DISA APLITS: **https://aplits.disa.mil/processAPList.do**), and configured IAW applicable guidance

3.20.4. RTS shall be assessed and authorized through the enclave that it is connected to according to DoD Cybersecurity RMF Process , **http://iase.disa.mil/diacap/**, and the RMF Knowledge Service, **https://diacap.iaportal.navy.mil/login.htm**.

3.20.5. Changes to Systems with an Established Authorization Decision.

3.20.5.1. After an authorization decision has been issued and a security baseline established (i.e., ATO), positive or negative changes to the system must be assessed by the system's ISSM to determine if the change has a security impact. The ISSM is critical in initiating the change review process. The ISSM will consult the SCA for an assessment of any change to the system to determine if re-authorization is required. If the

implementation of a cybersecurity control is affected by the change (especially for cybersecurity or cybersecurity-enabled products), there must be a validation of the cybersecurity control. This change may impact the authorization status, and the SCA must assess the implementation and validation of the cybersecurity control against functional and security guidelines. They will determine if system change does not affect the security baseline of the system, and that the residual risk level remains consistent with the current authorization.

3.20.5.2. If the ISSM determines the system change does not affect the security baseline of the system (i.e., no security impact (NSI)), the system may continue to operate under its current authorization decision. Changes are documented and included with the system security and C&A documentation. The ISSM will provide a synopsis of the NSI to the SCA for concurrence. If the SCA concurs or ASCA recommends and ACA concurs with the NSI, a new authorization decision and connection approval is not required. However, if the SCA does not concur with the NSI, the ISSM must take the actions identified in paragraph 3.20.5.3.

3.20.5.3. If the ISSM determines a change impacts the security baseline of the system, the SCA must evaluate the change and determine the appropriate course of action. If the SCA concurs the change impacts the security baseline of the system, and/or a weakness cannot be mitigated in a timely manner to bring the risk back to the level the AO accepted in the current authorization, a new authorization decision and connection approval is required. NOTE: If the change results in a new "High" or "Very High" (formerly known as a CAT I) vulnerability that can be corrected within 30 days or a new CAT II weakness that can be corrected/satisfactorily mitigated within 90 days, the system can continue to operate under the existing authorization decision and connection approval.

MICHAEL W. PETERSON, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 107-347, *E-Government Act*, December 2002; Title III, *Federal Information Security Management Act.*

National Institute for Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklist Users and Developers*, May 2005

CNSSI 4012, *National Information Assurance Training Standard for Senior System Managers*, June 2004

CNSSI 4013, *National Information Assurance Training Standard for System Administrators*, March 2004

CNSSI 4015, *National Training Standard for System Certifiers*, December 2000

DoDD 8100.01, *Global Information Grid (GIG) Overarching Policy*, 19 September 2002

DoDD 8500.01E, *Information Assurance*, 24 October 2002

DoDI 5000.2, *Operation of the Defense Acquisition System*, 12 May 03

DoDI 8500.2, *Information Assurance (IA) Implementation*, 6 February 2003

DoDI 8510.01, *Department of Defense Information Assurance Certification and Accreditation Process (DIACAP),* 28 November 2007

DoD 8570.01-M, *Information Assurance Workforce Improvement Program*, 19 December 2005

CJCSI 3170.01F, *Joint Capabilities Integration and Development System*, 1 May 2007

CJCSI 6211.02B, *Defense Information System Network (DISN): Policy, Responsibilities and Processes*, 30 Aug 06

CJCSM 3170.01C, *Operation of the Joint Capabilities Integration and Development System*, 1 May 2007

CJCSM 6510.01, *Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)*, 8 March 2006

AFPD 33-2, *Information Assurance (IA) Program*, 19 April 2007

AFPD 33-4, *Enterprise Architecting*, 27 Jun 2006

AFI 10-601, *Capabilities Based Requirements Development*, 31 July 2006

AFI 33-115v1, *Network Operations*, 24 May 2006

AFI 33-401, *Implementing Air Force Architectures*, 14 Mar 2007

AFI 63-101, *Operations of Capabilities Based Acquisition System*, 29 Jul 2005

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

AFSSI 8522, *Access to Information Systems*

DISA *Enclave* Security Technical Implementation Guide, Version 4, Release 2

IT Lean Guidebook, version 5.0, [pending release]

ACA Licensing Guide [pending release]

Table of IA Control Vulnerability Code Mapping [pending release]

Adopted Form

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

ACAT—Acquisition Category

AF Enterprise AO—Air Force Enterprise Authorizing Official (Previously AF-DAA)

AF SISO—Air Force Senior Information Security Officer (Previously AF SIAO)

AFCAP—Air Force Certification and Accreditation Program

AFCKS—Air Force Cybersecurity Knowledge Service

AFIN—Air Force Information Network (Previously AF-GIG)

AO—Authorizing Official (Previously DAA)

DODIN—Department of Defense Information Network (Previously GIG)

ISSM—Information System Security Manager (Previously IAM)

ISSO—Information System Security Officer

PIT—Platform Information Technology

PITI—Platform Information Technology Interconnection

SCA—Security Control Assessor (Previously CA)

SIP—System Information Profile

TAG—Air Force Certification and Accreditation Program Technical Advisory Group

AFCIO—Air Force Chief Information Officer

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

ANG—Air National Guard

E/APL—Evaluated / Approved Product List

ATC—Authorization to Connect

ATO—Authorization to Operate

C&A—Certification and Accreditation

CAR—Certifying Authority Representative

CCB—Configuration Control Board

CITS—Combat Information Transport System

CJCSI—Chairman, Joint Chiefs of Staff Instruction

CJCSM—Chairman, Joint Chiefs of Staff Manual

CL—Confidentiality Level

CNSSI—Committee on National Security Systems Instruction

CoP—Community of Practice

COTS—Commercial Off The Shelf

CSA—Computer System Administrator

CTM—Consent to Monitor

DAA—Designated Accrediting Authority

DATC—Denial of Authorization to Connect

DATO—Denial of Authorization to Operate

DIACAP—DoD Information Assurance Certification and Accreditation Process

DIP—DIACAP Implementation Plan

DISA—Defense Information Systems Agency

DITPR—DoD Information Technology Portfolio Repository

DITSCAP—Department of Defense Information Technology Security Certification and Accreditation Process

DNI—Director of National Intelligence

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DSAWG—Defense IA/Security Accreditation Working Group

E-ATC—Emergency Authorization to Connect

EITDR—Enterprise Information Technology Data Repository

FISMA—Federal Information Security Management Act

GO/SES—General Officer/Senior Executive Service civilian

GOTS—Government Off The Shelf

IA—Information Assurance

IATO—Interim Authorization to Operate

IATT—Interim Authorization to Test

IAW—In Accordance With

IS—Information System

ISO—Information System Owner

IT—Information Technology

JPD—Joint Potential Designator

MAC—Mission Assurance Category

MAJCOM—Major Command

OPR—Office of Primary Responsibility

PAA—Principal Accrediting Authority

PM/SM—Program Manager/System Manager

POA&M—Plan of Action and Milestones

PPS—Ports, Protocols, and Services

RDT&E—Research, Development, Testing, & Evaluation

SCAO—SIPRNet Connection Approval Office

SCQ—SIPRNet Connection Questionnaire

SCI—Sensitive Compartmented Information

SIAO—Senior Information Assurance Officer

SISSU—Security, Interoperability, Supportability, Sustainability, and Usability

STIG—Security Technical Implementation Guide

TAG—Technical Advisory Group

UCAO—Unclassified Connection Approval Office

UR—User Representative

VDD—Version Description Document

Terms

Acquisition Authority—The person responsible to sign a contract on behalf of the U.S. Government (e.g. Contracting Officer).

Air Force Provisioned Portion of the Global Information Grid—The AF-GIG is a system that provides a set of value-added functions operating in a global context to provide processing, storage, and transport of information, human interaction, systems and network management, information dissemination management, and information assurance. These functions must be fully integrated and interoperable with one another to achieve overall success across the AF-GIG. As a result, the AF-GIG is an information environment comprised of interoperable computing and communications components. The AF-GIG is part of the Global Information Grid (GIG). Therefore, the AF-GIG is the interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and

managing information on demand to warfighters, policy makers, and support personnel. The AF-GIG includes all owned and leased communications and computing systems and services, network operating systems, data, security services, and other associated services necessary to achieve information superiority. [AFI 33-115v1]

Authorization to Connect—The official AF-DAA approval for system connection to the AF-GIG. The AF-DAA assumes all risks associated with the connection of the system on the AF-GIG. Usually granted to systems where the acceptable residual risk after proper countermeasures and safeguards are implemented.

Connection—The process of establishing communication between ISs.

Denial of Authorization to Connect—AF-GIG DAA determination that an IS cannot connect to the AF-GIG because of an inadequate IA design, failure to adequately implement assigned IA Controls, or other lack of adequate security If the IS is already connected, the connection of the IS is terminated.

Enterprise IT Data Repository (EITDR)—The Air Force database of record for registering all systems and applications as required by public law and DoD directives. Registration in the EITDR is mandatory for all systems and applications developed by the Air Force, or for which the Air Force is the lead agency, or that requires connection to the AF-GIG. The EITDR is also the database of record for IT statutory and regulatory compliance. The repository contains compliance data for Information Assurance (IA), Internet Protocol version 6 (Ipv6), Public Key Enabling (PKE), Clinger-Cohen Act, etc. It is the primary data source for Federal Information Security Management Act (FISMA) reporting and the principal vehicle for gathering and storing system and application data to support planned and ad hoc data calls. The EITDR contains information about program management; system and application interfaces; networthiness; funding; Capital Investment Reports (CIRs) and other supporting data to facilitate IT portfolio management.

Information System (IS)—Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, display, or transmission of information.

NOTE:—The Air Force is adopting DoD cyberspace terminology from recently published DoDI 8500.01 and DoDI 8510.01.

Guest Information Systems—**Information** systems which do not follow the normal AFCAP requirements for C&A. They may follow other DoD or Federal C&A processes such as NIST 800-37, DCID 6/3. They also include other DoD Agencies which have performed DIACAP and are coming to the AF for connection to the Air Force provisioned portion of the GIG. These were formerly called Non-Air Force Information Systems.

Platform Information Technology (PIT)—A special purpose system which employs computing resources (i.e., hardware, firmware, and optionally software) that are physically embedded in, dedicated to, or essential in real time to the mission performance. It only performs (i.e., is dedicated to) the information processing assigned to it by its hosting special purpose system (this is not for core services).

Attachment 2

IA CONTROL EVALUATION METHOD AND VULNERABILITY SEVERITY CATEGORY ASSIGNMENT

A2.1. IA Control Validation Procedure Evaluation Method.

A2.1.1. The assigned DoD IA Controls are expected to be validated IAW the DIACAP Knowledge Service guidelines. Additionally, the following methodology will be used when performing and documenting IA Control validation procedures:

A2.1.2. There are four potential evaluation methods used while performing the validation procedures. They include:

A2.1.2.1. Interview (I) - provides an effective means of validating the results obtained with other methods. For example, an initial security training requirement may exist which is verified by inspection of training materials and documentation, but to validate the effectiveness of the training, interviews with users would be necessary. Interviewees also frequently provide more information than is initially asked of them, which ensures a more comprehensive validation activity By itself, the interview method in most cases is not appropriate, but when combined with another method, will give a better overall "picture" of the security environment.

A2.1.2.2. Document Review (D) - involves a review of descriptive documentation, a comparison of the appropriate characteristics with the defined security requirements, and a comparison with approved security specifications to verify conformance with the methodology applied. Reviews can also include the verification of accuracy and completeness of documentation or records.

A2.1.2.3. Observation (O) - is the physical observation of a predictable event, initiated by a specific input or set of inputs that will always yield the same output or response. Testers may use live or simulated data, actions, or a lack of action to stimulate the predicted response.

A2.1.2.4. Test (T) - is the collection, analysis and evaluation through systematic hands-on measurement under all appropriate conditions.

A2.1.2.5. The evaluation methods are listed in order of complexity and depth from least to most. If more than one method exists to validate an IA Control, the personnel performing the validation procedures should use the most in-depth method (more than one type may be used per control).

A2.1.3. The AFCAP TAG will review suggested evaluation methods and adjudicate any potential discrepancies with the approved types and post to the IA CoP.

A2.2. Vulnerability Severity Category Assignment

A2.2.1. DISA has provided guidance for assigning Vulnerability Severity Category Assignments, which the Air Force is adopting as the standard within the IT Lean process.

A2.2.2. The AFCAP TAG will review Vulnerability Severity Category Assignments, as suggested by DISA, and provide the final approved guidance in the AFCAP approved IA Control Evaluation Method and Vulnerability Severity Category Assignment Table. See AF IA CoP for the AFCAP approved IA Control Evaluation Method and Vulnerability Severity Category Assignment Table.