Air Force Certification and Accreditation Program (AFCAP)

Agent of the Certifying Authority (ACA)

Licensing Guide

Version 4

APPROVING/RELEASING AUTHORITY

AFCAP Agent of the Certifying Authority (ACA) Licensing Guide

APPROVED FOR RELEASE:

EFFECTIVE DATE: 18 June 2012
This Guide is effective immediately upon signature.

BRODIE.KENNETH.E.1038358975
Digitally signed by BRODIE.KENNETH.E.1038358975
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USAF, cn=BRODIE.KENNETH.E.1038358975
Date: 2012.06.26 15:47:26 -04'00'

_____

KENNETH E. BRODIE, GS-15, DAF
Air Force Senior Information Assurance Officer
Office of Information Dominance and
Chief Information Officer

Summary of Changes

Change	Version	Date
Initial Baseline Version	1.0	1 Oct 08
Added three new license types and expanded concept	2.0	1 Apr 09
Removed ACA license levels. Removed requirement for ACA Lead to be government. Removed references to specific organizations/office symbols. Changed ACA program roles, relationships, and responsibilities in general.	3.0	5 Jul 11
Reviewed for NETCENTS-2	3.1	16 Mar 12
Incorporates commercial ACAs and revises complete document	4	9 May 12

CONTENTS

EXECUTIVE SUMMARY

With the endorsement of the AF Senior Information Assurance Officer (AF SIAO), the Air Force Certifying Authority (AF-CA) has created the Agent of the Certifying Authority (ACA) construct to appoint licensed, qualified agents to provide accurate, consistent, and trusted AF Information System (IS) assessments. The licensed ACA acts as an independent trusted agent of the AF-CA, providing fact-based security analysis in support of the AFCAP. The ACA construct streamlines the validation process and enhances the overall effectiveness of the AF-CA. This construct will also promote the fielding of interoperable systems with optimum security features, countermeasures, and safeguards in place, on schedule, and without posing unacceptable risks to the AF Enterprise.

The ACA may be an individual, DoD / AF organization, or an industry partner and may consist of any combination of government and/or contractor personnel. The ACA will consist of an ACA Lead (and Assistant Lead) coupled with sufficient manpower, resources, and facilities. The Assistant Lead will assume the ACA Lead role in the absence of the ACA Lead. ACAs will be supported by appropriate resources, which may include facilities, ranging from small system testing locations to large scale facilities testing entire weapon systems. ACAs may often be required to travel to the location of the system. In addition, there are Special ACAs associated with supporting AF-level functional communities.

An ACA organization's services are contracted and funded by information system (IS) Program Managers (PMs) or IS Owners (ISO) to perform information assurance (IA) control validation services through a formal, documented agreement normally in the form of a task order. This document provides specific guidance for organizations performing ACA activities and PMs/ISOs who elect to use the services of licensed ACA organizations' services.

1. Introduction

1.1. **Purpose**

Provide guidance and processes on ACA licensing, including license preparation and application, evaluation of the license request, recommendation for award of a license, and maintenance of the license.

1.2.**References**

- Air Force Instruction 33-210, ***Air Force Certification and Accreditation (C&A) Program (AFCAP)***
- Department of Defense Directive (DoDD) 8500.01E, ***Information Assurance (IA)***
- DoD Instruction (DoDI) 8500.2, ***Information Assurance (IA) Implementation***
- DoDI 8510.01, ***DoD Information Assurance Certification and Accreditation Process (DIACAP)***
- DoDD 8570.01, ***Information Assurance Training, Certification, and Workforce Management***
- DoD 8570.01-M**,** ***Information Assurance Workforce Improvement Program***
- National Security Telecommunications and Information System Security Instruction 4015, ***National Training Standard for System Certifiers***

1.3. **Overview**

1.3.1. Inconsistent application/implementation of network and system security policies, countermeasures, and procedures may result in fielding systems with significant vulnerabilities, increasing the likelihood of unauthorized access. Vulnerable systems connected to the Air Force-provisioned portion of the Global Information Grid (AF-GIG) could expose the entire AF-GIG to unacceptable risks.

1.3.2. The AF Senior Information Assurance Officer (AF SIAO) has delegated the role of CA, for all AF ISs (excluding Space, SAP/SAR, and Intel) , to AFNIW/MW to perform security validations, conduct a risk analysis, and provide connection recommendations for systems seeking connection to the Air Force Enterprise Network (AFNet). The ACA provides certification determination recommendations to the AF-CA in support of accreditation and connection decisions, in accordance with the aforementioned references to increase the overall security posture of the IS and the AFNet.

1.3.3. In an effort to implement and execute C&A beginning with the acquisition process, the AF-CA has appointed Certifying Authority Representatives (CARs) to serve as an active member of each IS DIACAP Team to assist with planning of IA requirements. These personnel work with the PM and DIACAP team to ensure the implementation and validation procedures are performed as identified in the DIACAP, on behalf of the CA, if the validation activities are not contracted to an ACA. If contracted to an ACA, the ACA participates on the DIACAP Team and the CAR acts as an administrative authority to verify artifacts have been properly documented in

eMASS before forwarding the C&A package to the AF-CA for certification determination.

1.3.4. To increase process effectiveness and efficiency for testing and/or validation of IA controls, the AF-CA, with approval from the AF SIAO, created the ACA construct and using this licensing process, will license ACAs to perform testing and validating functions of the AF-CA for IS IA controls from an organizationally independent perspective. ACA's shall perform comprehensive evaluation of the technical and non-technical IA controls of an IS, determine the degree to which the IS meets its specified security requirements, and provide mitigation recommendations. The ACA's position of independence from the acquisition/program office and operations community lends credence and validity to the AFCAP.

1.3.5. In some cases AF functional communities use ISs employing unique technologies, capabilities, or security implementations. The AF SIAO has delegated CA responsibilities for these functional communities; examples include medical systems, logistics systems, and Research, Development Test & Evaluation (RDT&E), Science & Technology systems AND Platform Information Technologies (PIT). These functional communities may submit an individual, organization, or industry partner for a Special ACA license. These specialized licenses are limited in nature but allow the AF-CA to capitalize on the Special ACA's inherent specialized knowledge of the functional community's systems to further increase efficiency and assessment accuracy.

1.3.6. The ACA will be contracted by a Government organization to assist in certification activities and shall meet and maintain the intent of DIACAP's independence between the program office, the individuals developing an IS, and where applicable, those individuals implementing and testing security controls. In an ACA's full capacity, they are testing and validating the security controls implemented by the IS development team, Information Assurance Manager (IAM)/Information Assurance Officer (IAO) personnel and DIACAP team. The ACA's position of independence from the acquisition/program office and operations community lends credence and validity to the AFCAP. Utilization of commercial ACAs (industry partners) shall be a separate task order under SAF/AQ and SAF/CIO mandatory use of Network - Centric Solutions (NETCENTS) contracts.

1.3.7. The work of a licensed ACA is dependent on the continuous work of an IS development team, and where applicable, the respective IA Team and its IAM/IAO. Typically, the IAM is responsible for managing the IA program of an IS within a network environment. Incumbents in these positions perform a variety of security related tasks, including the development and implementation of system information security standards and procedures. They also maintain situational awareness and initiate actions to improve or restore IA posture as well as conduct annual security reviews of all IA controls and a test of selected IA controls. If an independent IAM is not assigned to an IS, the ACA may fulfill this role as well as the validation role.

The figure below highlights the ACA C&A model to be used by licensed ACAs. Currently, government/contractor personnel appointed as a CARs at the AF-CA attempt to work in tandem with the geographically separate PM and IAM/IAO of an IS to ensure IA controls are implemented properly throughout the acquisition and development of an IS. While this provides a theoretically ideal model for C&A by considering DIACAP activities while implementing IA controls, there is significant resource challenges based on the volume of ISs requiring certification activity at the AF-CA. As a result, ACAs (to include qualified licensed commercial entities), are required to assist the AF-CA in the validation phase to increase efficiencies in the process under the ACA C&A model.

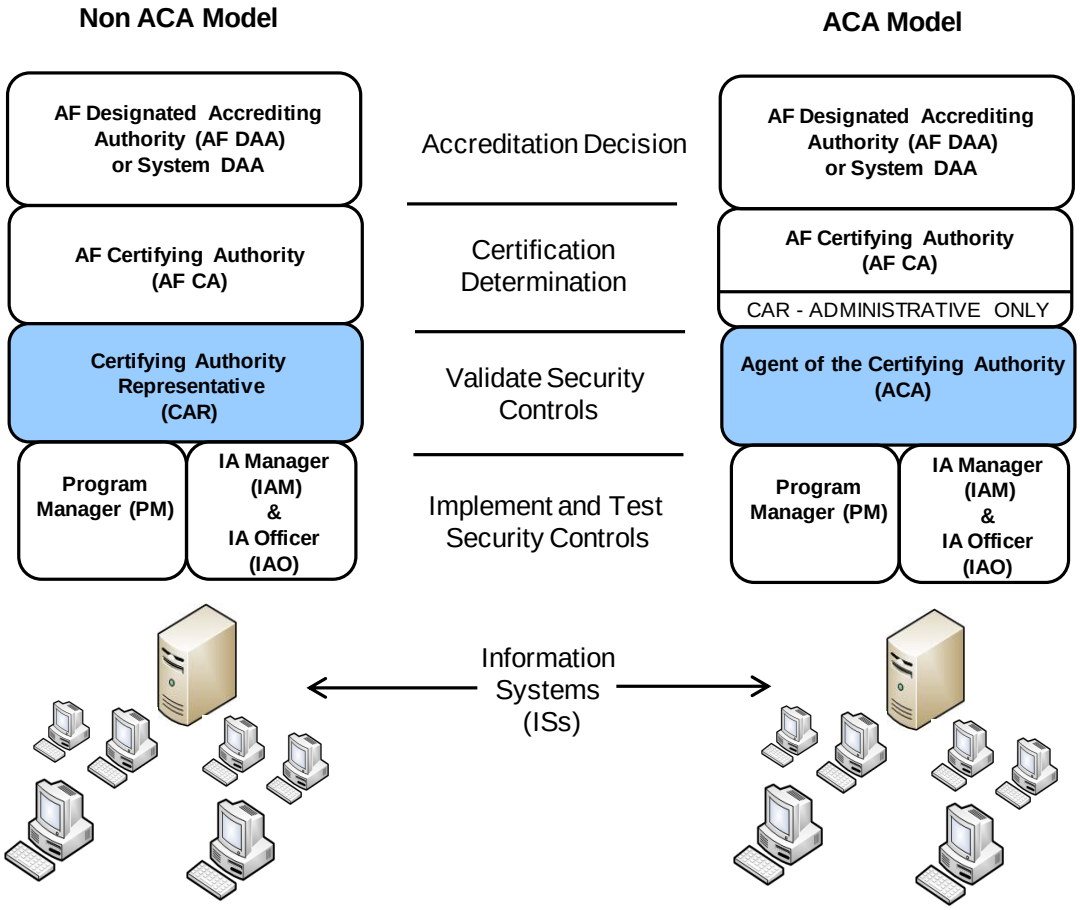

FIGURE 1: ACA Certification & Accreditation Model

2. Scope and Applicability

2.1. The number and complexity of ISs in the AF make it necessary for the AF-CA to license qualified entities as ACAs to test and validate IA control compliance in support of a certification recommendation. As a minimum, the ACA performs hands-on validation as described in DoDI 8510.01 to assess the effective implementation of IA controls and other security requirements, based primarily on the validation procedures on the DIACAP Knowledge Service (DIACAP KS. However, the ACA may identify, validate, and assess

security weaknesses by additional means. Regardless of how the vulnerabilities are identified, the ACA recommends how to fix or mitigate security vulnerabilities. The validation of IA controls solely through the review of system artifacts is insufficient; rather, the ACA must perform hands-on testing of system security features, as well as witness first-hand, through facility visits, the actual processes related to each IA control, whether the controls are technical, personnel, operational, or management in nature. Most importantly, the ACA role in the C&A process ensures an objective approach to the validation of IA controls while providing an accurate perspective of a system's IA posture. ACA validation activities will be primarily performed on a fee-for-service basis. Per AFI 33-210, para. 2.11.7, while PMs fund ACA's support to the program, the ACA must remain independent of the program office and is solely accountable to the CA for the accuracy of all validation products.

2.2. This ACA licensing guide is applicable to organizations performing, or seeking a license to perform, ACA activities and to PMs who elect to use the services of licensed ACA organizations. ACA services may be used for all AF IS (i.e. Automated Information System applications, enclaves, outsourced IT-based processes, PIT, PIT Interconnections), to include stand-alone systems. This ensures IA for all ISs procured for the AF and operated on the AFNet are consistent with Federal, DoD, and AF policies and a standardized and independent certification approach is maintained. ACAs will validate proper implementation of IA controls as required by DoDI 8500.2, AFI 33-210, the DIACAP Knowledge Service (KS), etc. AF IT requiring validation include, but are not limited to, the following, whether networked or stand-alone:

- New or non-accredited AF IS
- Previously accredited AF IS requiring re-accreditation
- New AF circuit-enclaves (Base Local Area Networks)
- Previously accredited AF circuit-enclaves requiring re-accreditation

3. Roles and Responsibilities

3.1. The AF SIAO, in accordance with DIACAP, is the Air Force Certifying Authority, for all Air Force IS (excluding Space, SAP/SAR, and Intelligence systems). The AF SIAO can delegate certifying authority as required and has delegated CA duties to AFNIC/NW but maintains overall responsibility. The AF SIAO is the sole authority for disapproval of ACA license requests and revocation of ACA licenses. Disapprovals and revocations will be issued in writing.

3.2. AF-CA Requirements and Responsibilities:

3.2.1. Review all ACA licensing requests and either approve licensing requests or recommend ACA license disapprovals to the AF SIAO.

3.2.2. Maintain a list of licensed ACAs.

3.2.3. Conduct teleconferences with the ACA Leads to discuss overall ACA efforts, quality, problems, situations, trends, and other issues as needed. Elevate unresolved issues to the AF SIAO as required.

3.2.4. Recommend to the AF SIAO revocation of the ACA license of any ACA which repeatedly fails to follow the AFCAP ACA Licensing Guide or ACA PM guidance.

3.2.5. Review ACA C&A products (as components of the overall C&A package) to ensure continued quality of the ACA's products over time.

3.2.6. Issue the final certification determination. The AF-CA signs the certification determination, provides the Air Force Designated Accrediting Authority (AF DAA) with assurance of the certification, and identifies residual risk to support an accreditation decision.

3.2.7. Monitor ACA performance metrics and provide quarterly ACA reports to the AF SIAO to include current versions of all ACA MOAs.

3.3. ACA PM (Air Force Network Integration Center, Networthiness Division (AFNIC/NW) Requirements and Responsibilities:

3.3.1. Provide the ACA with the ACA Licensing Guide, licensing request package templates, and assistance as required.

3.3.2. Update the ACA Lead with any/all changes to validation procedures, documentation requirements, or AF-CA/AF DAA processes in an "ACA System Program Update" email at least monthly.

3.3.3. Be available to answer or help the ACA Lead as required.

3.3.4. Conduct meetings or teleconferences with the ACA Leads or Assistant ACA Leads to discuss the ACA issues on an as-needed basis.

3.3.5. Elevate problems, issues, or situations that cannot be resolved with the ACA Lead to the AF-CA or AF SIAO as required.

3.3.6. Send MOA change requests to AF-CA for approval.

3.3.7. Review final ACA certification determination recommendations/packages for compliance with current standards and requirements prior to submission to the AF-CA. Resolve all issues with the ACA Lead.

3.3.8. Provide quarterly updates to AF-CA and AF SIAO on ACA activities and health of ACA program compiling quarterly ACA Lead metrics reports.

3.4. The ACA Lead is ultimately responsible to the AF-CA and shall:

3.4.1. Maintain professional currency in the IA field, IA certification and assessment methodologies, and the technology field (i.e., Computing Environment certifications),

as required by DoDD 8570.01. The ACA Lead and Assistant Lead shall possess and maintain an Information Assurance Manager (IAM) Level III certification.

3.4.2. Maintain the highest level of personal and professional ethics.

3.4.3. Maintain total independence from the Program Management Office (PMO) and/or the IS developer.

3.4.4. Renew the ACA license annually per paragraph 8 below.

3.4.5. Prepare and maintain appropriate MOA, resumes, diagrams, topologies, and other documentation consistent with licensing application package (see Appendix "C" for MOA template).

3.4.6. Maintain a qualified and trustworthy ACA staff, compliant with DoD personnel security standards and DoDD 8570.01 licensing requirements, to perform IA control validation services for IS PMs.

3.4.7. Provide PMs a written estimate to identify the manning and resources necessary for the level of validation effort requested by the PM and all associated costs.

3.5. IS PMs who choose to use a commercial ACA, through the applicable Information System Owners (ISOs), are responsible to:

3.5.1. Execute a documented agreement to contract the ACA's services to perform IA control testing and/or validation. Ensure the specific certification requirements, desired capabilities, and required validation tasks are detailed in the documented agreement or PWS. The NETCENTS performance work statement (PWS) will include basic language that can be tailored to meet this requirement. The documented agreement or PWS may include other requirements or tasks required such as IAM/IAO support, but cannot include the development or sustainment of the IS.

3.5.2. Plan/program for and fund the ACA activity as part of the ISC&A lifecycle. While PMs fund and coordinate ACA activities, the ACA is solely accountable to the CA for the accuracy of all validation products. Functional communities or other domains may fund for Special ACAs to support their entire mission or portfolio area.

3.6. Information Assurance Managers (IAM) and Information Assurance Officers (IAO). If present in the program, the IAM 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 DIACAP, IAMs and IAOs assigned to Air Force ISs will complete and maintain appropriate IA certification IAW DoD 8570.01-M.

4. ACA Validation Responsibilities.

The ACA must be an active participant during the entire C&A process. The ACA entities possess the capability to perform both testing and validating functions of IA controls, functions that may potentially overlap with existing IAM/IAO personnel functions assigned to an IS. Thus, there are two different scenarios that would employ an ACA with differing responsibilities.

In the first scenario, it is assumed that the Program Office has personnel independent from the system developer and the control of the PMO to fill IAM/IAO positions to implement and test the IS security controls. In this case, the Program Office would need to seek an independent authority, an ACA, to **validate** the testing of the IAM/IAO personnel before the AF-CA signs off on the IS.

In the second scenario, it is assumed that the Program Office has not staffed independent IAM/IAO positions to implement and test security controls in tandem with the IS developers. In this case, the Program Office would need to seek an authority independent of the program, again an ACA, to perform both **testing** and **validating** of any existing IS security controls put in place by the IS developers. If mitigations to remaining IS vulnerabilities were required, the ACA would possess the necessary skills to recommend additional security controls for program personnel to implement so that the ACA could subsequently re-test and validate.

Throughout the C&A process, ACA activities and deliverables include, but are not limited to, the following:

4.1. Enter into a documented agreement (i.e. Service Level Agreement (SLA), MOA, Project/Program Support Agreement (PSA), PWS, etc.) on the scope and level of effort for ACA support with the IS PM before any activities begin. The agreement will include, but is not limited to, specifics on:

4.1.1. Validation activity dates.

4.1.2. Validation activity prerequisites.

4.1.3. Appropriately specified DoDD 8570.01 certification levels for all test team members applicable to the system under test.

4.1.4 Review of IS IAM/IAO qualifications, security plans, applicable security artifacts.

4.1.4. List of hardware, software, test tools, and/or other test resources provided by the PMO or ISO.

4.1.5. List of hardware, software, test tools, and/or other test support resources provided by the system PM.

4.1.6. System IA controls validation to be completed.

4.1.7. ACA reports and documentation delivered to system PM.

4.1.8. Format requirement and delivery timelines for each report and document.

4.1.9. ACA and IS PM responsibilities.

4.2. Perform activities in the documented agreement with the PM, which may include, but are not limited to:

4.2.1. Help determine the appropriate Mission Assurance Category and Confidentiality Level of the IS.

4.2.2. Help tailor the baseline IA controls. Ensure common understanding of IA control requirements and DIACAP KS validation procedures.

4.2.3. Review design proposals to determine compliance with established IA control implementation guidance requirements through all phases of system engineering.

4.2.4. Develop an IA Test Plan (as a component of the Test and Evaluation Master Plan) to inform the PM of which requirements will be tested and the test methodologies.

4.2.5. Help the PM develop the System Identification Profile (SIP), and evaluate the System Identification Profile (SIP) (on behalf of the AF-CA).

4.2.6. Help the PM develop the DIACAP Implementation Plan (DIP), and evaluate the DIACAP Implementation Plan (DIP).

4.2.7. Evaluate logical system diagrams or system topologies for accuracy and completeness.

4.2.8. Help select and evaluate Ports, Protocols, and Services.

4.2.9. Prepare IA control validation plans in accordance with (IAW) the validation procedures on the DIACAP KS.

4.2.10. Perform hands-on validation of IA controls IAW DoD IA requirements, including technical system evaluations/testing IAW Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), National Security Agency (NSA) Configuration Guides, automated scripts/tools to include source code scanning tools (e.g. DISA Gold DiskFortify, eEye Retina), and or any other testing requirements outlined in the documented agreement4.2.11. Review and provide input to all system artifacts to determine compliance with all IA controls.

4.2.12. Assist in resolving weaknesses identified during validation.

4.2.13. Re-validate IA controls to ensure identified vulnerabilities of the IS are in fact resolved.

4.2.14. Prepare artifacts to support and convey the IA controls actual validation results.

4.2.15. Evaluate and/or help prepare the DIACAP scorecard.

4.2.16. Evaluate and/or help prepare Plans of Action and Milestones, including developing/recommending mitigations and potential fix actions for remaining vulnerabilities.

4.2.17. Ensure all required artifacts are available to the PM such that the PM may enter the comprehensive DIACAP package into the AF IS C&A tool of record for review. In specified circumstances, the ACA may be requested to input IS artifacts in eMASS.

4.2.18. At the request of the IAM (as part of the Configuration Control Board function), assess changes to the IS to determine the impact to the system's IA posture.

4.2.19. At the request of the IAM, perform annual evaluation and validation and/or testing of select IA controls.

4.3. Provide the IS PM with detailed documentation, to include:

4.3.1. IA controls validation activities completed.

4.3.2. IA control validation results.

4.3.3. Analysis of how to correct or mitigate security vulnerabilities.

4.3.4. Any other requirements in the documented agreement (i.e. SLA, MOA, PSA, PWS, etc.) with the system PM.

4.4. Provide the AF-CA and/or ACA PM with all system documentation as requested in writing.

4.4.1. All documentation prepared in support of and/or resulting from ACA validation activities are the property of the government and may not be considered proprietary, in accordance with the Federal Acquisition Regulation (FAR) Part 27.

4.4.2. All agreements and contracts with ACAs will be written in such a manner as to ensure all documentation shall be made available to the government.

4.5. Provide completed certification determination recommendations and applicable assessments of IS residual risk to the AF-CA. All documentation, recommendations, and assessments will be reviewed by the ACA PM to ensure compliance with current standards and requirements. Issues identified during review will be returned to the ACA Lead for rework and/or resolution.

4.6. Provide quarterly status reports to the ACA PM on the current IA activities of the ACA. The report is due 10 business days following the end of the quarter, based upon Federal Government fiscal calendar. ACA PM will provide copies of the report to the AF-CA and AF

SIAO. The report will be formatted IAW the template provided by ACA PM and will include the following:

4.6.1. List of systems being validated, status, and estimated completion date.

4.6.2. List of systems in the queue, date of contract/agreement, and estimated start date.

4.6.3. Major negative trends (within or across ISs) associated with system testing including trend description, impacts, and solutions.

4.6.4. Major issues affecting IA control validation including description, impact, and solutions.

4.6.5. Undue influence or pressure applied by the IS PM, IAM, ISO, developer, etc.

4.6.6. Changes that may impact ACA license eligibility. Describe, as a minimum, issues that:

4.6.6.1. Impact evaluation, testing, or validation.

4.6.6.2. Impact ability to perform responsibilities as outlined in the ACA Licensing Guide or MOA.

4.6.6.3. Create any conflict of interests, and mitigation efforts or plans to resolve those conflicts.

4.6.6.4. Change of key personnel (ACA Lead, test team leads, etc.) eligibility, to include position, qualifications, security clearances, certification requirements, resumes, etc.

5. Licensing Requirements

5.1. There are two types of ACA licenses, General and Special. The activities of both are the same, but Special ACAs are different in that they support a specific mission area.

5.2. The ACA Lead, Assistant ACA Lead, ACA team leaders, and ACA support personnel may be government, contractor, or a mix of government and contractor personnel. ACA staff composition shall be documented during the ACA application process and updated and reported to the ACA PM as team composition changes. The AF-CA must have an understanding of and confidence in the ACA's ability to handle system certification testing.

5.3. The ACA Lead and Assistant Lead will:

5.3.1. Ensure ACA Lead and staff continuity and knowledge of AF IS and IA status and issues.

5.3.2. Ensure the highest level of integrity within the ACA's organization and the C&A process.

5.3.3. Ensure he/she/they is/are the only person(s) authorized to sign on behalf of the organization licensed as the ACA.

5.3.4. Be accountable to the AF-CA, who must have trust and faith in the ACA's validation results.

5.4. The ACA Lead and Assistant Lead must meet the following requirements:

5.4.1. Be a U.S. citizen.

5.4.2. Hold a U.S. Government security clearance and formal access approvals commensurate with the level of information processed by the IS(s) under his/her purview as an ACA or a Secret clearance, whichever is higher.

5.4.3. Maintain a current Single Scope Background Investigation

5.4.4. Have the necessary breadth and depth of IA knowledge to perform IA controls validations. This is demonstrated by obtaining and maintaining a DoD 8570.01-M IAM Level III certification, See Attachment A, Table A-1.

5.4.5. As a minimum, have 8 years of high-level (enterprise-level preferred) IT experience, with a minimum of 5 years of senior-level experience in IA. In addition to the years of experience, the following must also be discernable from the resume:

5.4.5.1. Comprehensive understanding of DoD and AF IA policy.

5.4.5.2. Practical application of IA through security engineering, security test and evaluation, or project IA positions.

5.4.5.3. Knowledge and judgment necessary for making proper evaluations of threats, vulnerabilities, and risks and understanding them in the context of their likelihood of exploitation.

5.4.5.4. Support the goals and needs of the AF-CA and the AF-GIG with a Defense-in-Depth view combining IA principles with technological best practices in the best interests of the AF.

5.5. ACA Team Requirements:

5.5.1. While there is room for many specialties within the IA field, the ACA as a whole must maintain a mature, holistic, and balanced view toward IA and the AF Network that blends a thorough understanding of the nature of technology, security, the enterprise, and operational needs.

5.5.2. There are no restrictions to an ACA organization's size, nor are there limitations to the volume and type of work. The team supporting the ACA Lead must comply with requirements outlined in the application.

5.5.3. Some ACAs may specialize in certain technical fields and, thereby, be more efficient at assessing IS using that technology than other ACAs possessing a more general capability.

5.5.4. All ACA support personnel in technical positions (i.e. testers, technical writers, validators, etc.) must have and maintain the necessary breadth and depth of IA knowledge to perform IA control validation. This will be demonstrated by obtaining and maintaining a DoD 8570.01-M IAT or IAM Level I, II, or III certification commensurate with the type of system being tested or validated (i.e. Level I (computer environment (stand alone system/desktop)), Level II (networked environment (base/local network)), and Level III (Enterprise environment)). Commercial certifications meeting the requirements for DoD 8570.01-M Computer Network Defense Auditor are also acceptable. Per DoD 8570.01-M, para. C3.2.4.8.3, ACA team members who require privileged access to execute test tools or configuration checks must obtain the appropriate Computing Environment (CE) certifications for the operating system(s) and/or security related tools/devices they support in addition to the baseline IA certification requirement for their level. If the tester lacks a CE certification for the system or device under test, the PM or IAM may require a system administrator run the test tool or oversee manual system configuration validation. See Appendix A, Table A-1 for certification requirements.

5.5.5. The requiring agency (ISO, IS, MAJCOM, PEO) may also require IAM/IAO support to fulfill the roles for an IS or a group of ISs. This person(s) would support and receive program guidance from the IS Program Manager and not from the ACA though the two would interact based on the security roles they both perform. Acquiring IAM support also falls under the scope of the NETCENTS-2 Application Services contracts and could be included in the ACA task order or could be a separate task order.

5.6. Special ACAs must meet the above requirements for a General ACA, except Special ACAs must also demonstrate specific experience and knowledge of IS in the functional area they plan to support. Functional DAAs or CAs must concur with all Special ACA license requests within their communities prior to the ACA being issued a license by the AF CA. Functional DAAs or CAs may modify or augment the required qualifications for Special ACAs with the approval of the AF-CA.

6. Business Rules

Appointment as a licensed ACA does not guarantee the ACA will receive work. For commercial ACAs, the system PM, through the ISO, has the responsibility to comply with AF Mandatory Use Policy and use the NETCENTS contract vehicle to solicit a commercial ACA that best meets the AF and Program needs, generally driven by cost and schedule. To ensure all ACAs provide consistent and standard quality, work, cost, and schedule estimates consistent in breadth and depth with other ACAs, the following apply:

6.1. The DoD published standard validation procedures for each DoDI 8500.2 IA control and the expected results constitute compliance. These validation procedures, located on the

DIACAP KS at https://diacap.iaportal.navy.mil, will be used by the ACAs during validation of DoDI 8500.2 IA controls. ACAs must verify the system's compliance with AFI 33-210 requirements, STIGs, and applicable DoD policy. There will always be assumptions made by the ACAs as to needs, and this will affect the cost and schedule quote they provide to the PM. The ACAs must be as comprehensive and thorough as possible in detailing assumptions and activities when providing quotes to the PM.

6.2. Independence is the cornerstone of the ACA construct and their findings must remain independent and free from external influences. ACAs will not exhibit favoritism toward closely related units. ACAs will be independent from the system developer and PMs to ensure the most objective validation information is provided to the AF-CA. Violations of these important tenets can result in license revocation.

6.3. The General ACA must provide services to anyone on an impartial basis, based on availability. Organizations may not establish an ACA for their exclusive use by not accepting requests from other units or agencies. This arrangement undermines the ACA program's foundational tenet of independence.

6.4. Special ACAs are different in that they are intended to support a specific mission area (e.g. Medical Community, RDT&E, .edu, PIT, etc) and, therefore, are authorized to provide services only for systems within their area of expertise. However, Special ACAs are still required to maintain independence from a specific PMO and to provide services to anyone in their community of expertise on an impartial basis.

6.5. Coordination between the ACAs, ACA PM, and the AF-CA is a key factor in the success of the C&A process.

6.6. The ACA lead will expeditiously report to the AF-CA any validation situations potentially resulting in an unfavorable certification determination. The ACA Lead and the Program Office will take corrective action to alleviate or mitigate the problems. ACA Leads or PMs may bring issues/conflicts with test methodologies, test results, and or ACA / PM conduct to the ACA PM who will elevate it to the AFCA as needed. The plan of action will be reported through the ACA PM to the AFCA.

6.7. ACA organizations are encouraged to collaborate with other ACAs to take advantage of specialties, capabilities, and proven best practices. When ACAs do collaborate, the original ACA Lead is responsible for the overall certification effort and reporting. All certification work should result in the same level of evaluation and similar results. The difference between ACAs' cost and schedule estimates will be based generally on efficiency of process, temporary duty costs, and availability of personnel to perform the mission. The work product should result in the same level of assurance, regardless of which ACA is used.

6.8. Whether or not a system receives a positive certification determination and an accreditation recommendation is based solely on the IA posture of the IS and is the final decision of the AF-CA. While the quality of testing, validation, findings, and perceptions of the ACA play a role, the authority to provide a certification determination lies solely with the AF-CA, not with the ACA.

6.9. An ACA not following the AFCAP ACA Licensing Guide and/or violating the independence tenet will have their license revoked by the AF SIAO. The affected ACA may appeal to the AF SIAO for reconsideration of the revocation by preparing a letter of request with supporting documentation, verifying the violation(s) are corrected.

6.10. ACAs will work with the system program manager and/or information system owner to ensure proper utilization of the AF Enterprise Mission Assurance Support System (eMASS) to support C&A workflow activities.

7. ACA Application and Approval Process

7.1. A person or organization cannot advertise themselves as an AF-licensed ACA until their application has been approved and the AF-CA issues an ACA license.

7.2. Contractors on the NETCENTS-2 Application Services Contracts (Either the unlimited or the small business set aside) will be provided guidance on when to initiate the licensing process from the NETCENTS-2 team at the Post Award conference in Spring 2012. The contractor will then provide the information listed in the ACA Application, Table 8-1, and send the complete application, with all required supporting documentation to the ACA PM for evaluation All non-fulfilled requirements must be fully explained, accompanied with a written plan for compliance with milestones, and justification why ACA licensing should be considered.

7.3. The ACA Lead will pre-coordinate all ACA initial and renewal licensing request packages through the ACA PM. The ACA license request package pre-coordination process is completed before licensing packages are processed for approval and MOA signature. The ACA PM will review and return the ACA Licensing Request package to the ACA Lead within 5 working days. This process will save time and reduce the number of packages submitted to senior leadership.

7.4. The AF-CA will make the determination to approve an ACA licensing request package and will sign the ACA MOA and ACA license. All ACA license request disapprovals must be rendered by the AF SIAO.

7.5. The ACA PM will return a copy of the AF-CA-signed ACA MOA and license to the ACA Lead.

7.6. The ACA Lead will immediately notify the ACA PM of any changes to the information upon which their appointment decision was made, or which adversely affects their ability to perform the ACA function. This may include but is not limited to:

7.6.1. Changes in the supporting organization that significantly reduce the technical or IA qualifications of the supporting team.

7.6.2. Changes in the duties of the ACA Lead within the organization that might affect the ACA Lead’s ability to perform ACA duties.

7.6.3. Conflicts of interest associated with specific ISs or projects that would disqualify the ACA Lead personally or the ACA as a whole from certain functions.

7.6.4. Personal issues that no longer allow an ACA Lead to perform as an ACA, for example, illness, death, change in duty position, etc. If the organization wishes to continue its role in support of the ACA, the ACA Assistant Lead will assume the ACA Lead role until a new ACA Lead request application is submitted and approved. The approval process will begin again with notification and application of a new ACA Lead showing compliance with the stated requirements. The Assistant ACA Lead will continue the Lead ACA role until a new ACA Lead is approved. NOTE: The ACA Assistant Lead may remain in the Lead role for 180 days before the ACA would be subject to license revocation.

8. Annual ACA License Recertification:

8.1. The ACA will recertify annually (12 months from the date the ACA license was issued) to ensure they are maintaining compliance with policies, standards, and personnel certification requirements. The ACA Lead will submit the license renewal package to the ACA PM 6 weeks prior to the license expiration date to prevent the current license from expiring. This allows 2 weeks for ACA PM review, 2 weeks for AF-CA staff review, and 2 weeks for AF-CA review and signature. Failure to provide a complete ACA license renewal request package to the ACA PM 6 weeks prior to the current license expiration date may cause the current ACA license to expire before a new license is signed.

8.2. If the ACA license expires due to action or lack of timely action on the part of the ACA, the ACA PM will notify the AF-CA and request further guidance. The ACA will be removed from the list of licensed ACAs. The license will expire on the expiration date, and the ACA will be required to apply for an initial ACA License.

8.3. ACAs shall review their validation policies, procedures, and practices during annual license renewal. This review will address all new requirements and changes as related to licensing, validation, certification, and accreditation. This review will determine the continued applicability of their policies, address any necessary modifications, and provide an opportunity to incorporate lessons learned into their policies and procedures.

8.4. The ACA license renewal package contains required documentation to support all requested changes to the original ACA application and a new MOA. The ACA Lead will coordinate the new MOA with the ACA PM before the package (including the MOA) is signed. The ACA license renewal package request follows the same process as the original application. A signed ACA license and MOA will be issued to the ACA when the AF-CA approves the renewal license package request.

8.5. All ACA personnel are required to stay up to date on current tools, testing techniques, and certifications. The ACA will budget and provide for annual training classes, conferences, etc. where security testers can update and refresh their skills and comply with continuing education requirements to maintain certifications. Personnel information will be updated and

reported during annual license renewal and quarterly as changes are made to the initial licensing request package.

8.6. Document all policy, procedural, and training reviews along with the submission of the ACA Recertification Memo (Appendix A, Item 3b), as part of the annual license renewal request.

8.7. Failure to complete this license renewal process before the expiration date on the license will result in automatic revocation of the license.

8.8. The AF-CA will make the determination to approve an ACA licensing request package and will sign the ACA MOA and ACA license. All ACA license request disapprovals and revocations must be rendered by the AF SIAO.

8.9. The ACA PM will forward a copy of the AF-CA-signed ACA MOA and license to the ACA Lead.

8.10. The AF-CA may recommend to the AF SIAO revocation of an ACA license if the ACA organization repeatedly does not follow the AFCAP ACA Licensing Guide, ACA PM guidance, or AF-CA guidance.

8.11. The ACA Lead may appeal to the AF SIAO for reconsideration of the license revocation.

ACA Application	
#	**Requirements**
1	Provide name, rank, organization, location, and contact information of ACA Lead and Assistant Lead.
2	Confirm U.S. Citizenship (Yes/No) of ACA Lead and Assistant. State other countries of which you are a citizen:
3	Provide security clearance information (minimum Secret Level clearance or highest system classification level processed, whichever is higher) of ACA Lead, Assistant ACA Lead, and ACA designated team leads, and list any special access. Clearance information (investigation type, date, and agency conducting investigation) must be documented and signed by the ACA's local Security Manager or equivalent.
4	Provide resumes of the ACA Lead, Assistant ACA Lead, and other designated team leads supporting the ACA Lead identifying compliance with the requirements as follows:
4a	List all formal IA certifications. See Appendix A, Table A-2. for examples of IA certifications. Provide applicable certificates. ACA Lead and Assistant ACA Lead require IAM Level III certification or equivalent – see Appendix A and DoD 8570.01-M for details.
4b	Resumes must provide evidence of IT experience, IA years of experience, and certifications. ACA Lead and Assistant ACA Lead – Minimum 8 years of high-level (enterprise-level preferred) IT experience with 5 years of senior-level IA experience. Team leads – Minimum 5 years IT experience. All resumes must provide evidence of basic experience/skill requirements as detailed in DoD 8570.01-M Chapter 3 and 4 and IA certifications.
5	Provide list of all support personnel and their information. See template at Appendix

	A, Table A-3 in this guide
6	If the ACA Lead is government and employs contract personnel, provide a copy of the contract and a list of all contract deliverables.
7	Provide a description of the system testing facility environment to include layout, architectural drawings, diagrams, topologies, and network boundaries.
8	The Government will provide ACA test facility plans to the PM to demonstrate evidence and documentation of capabilities for replicating or emulating typical Local Area Network and/or Wide Area Network (WAN) environments found on AF installations, as well as AF Enterprise network and lower speed tactical network environments. Commercial ACA's have the inherent obstacle of replicating such environments due to the security posture required by IC, DoD and AF requirements, and as such must use existing government test facilities. Some of these facilities include the Defense Information Systems Agency (DISA), the Capabilities Integration Environment (CIE), the Command &Control (C2) Lab, the 46th Test Squadron (TS), and the Medical Lab. CIE, TIF, CEIF, and 46 TS DTF
9	The Government will provide information on the test facility to be used. The ACA shall provide evidence and documentation of personnel capabilities for testing and evaluating the security of subject IS on a closed network not further connected to the organization, installation, or WAN.
10	Provide evidence and documentation of the physical security capability to process and secure vulnerability, risk, and threat data. State highest authorized classification level (minimum is SECRET). For traveling ACAs, provide evidence and documentation of physical security capability to appropriately protect data accumulated by the ACA during travel and ensure it can be properly transported for further processing.
11	Provide a copy of the IA testing policy and plan, with a repeatable methodology, and individual roles and responsibilities.
11a	Provide description, explanation, and evidence with documentation of official plans for IA test, i.e. approach for testing, rules of engagement, compliance with legal issues, and policy issues.
11b	Provide evidence and documentation of plans to safely and effectively execute an information system test (e.g., to prevent "collateral damage" to network/systems while completing the test, to ensure different test procedures for testing on operational networks, and to ensure appropriate authorities and mission owners are identified and notified of test activities).
11c	Provide evidence and documentation of plans to appropriately handle data (collection, storage, transmission and destruction) throughout the testing process.
11d	Provide evidence and documentation of plans to conduct analysis and reporting to translate findings into risk mitigation actions to improve the information system security posture.
12	Provide documentation of all types of certification activities the ACA desires to support. This documentation must also specify each area of specialized technologies, functional areas, geographical areas, or in support of specific Commands or projects.

Table 8-1. ACA Application Requirements Checklist

Appendix A -Certifications and Reporting Requirements

1a. Excerpt from DoD 8570.01-M Table AP3. T2. DoD Approved Baseline Certifications

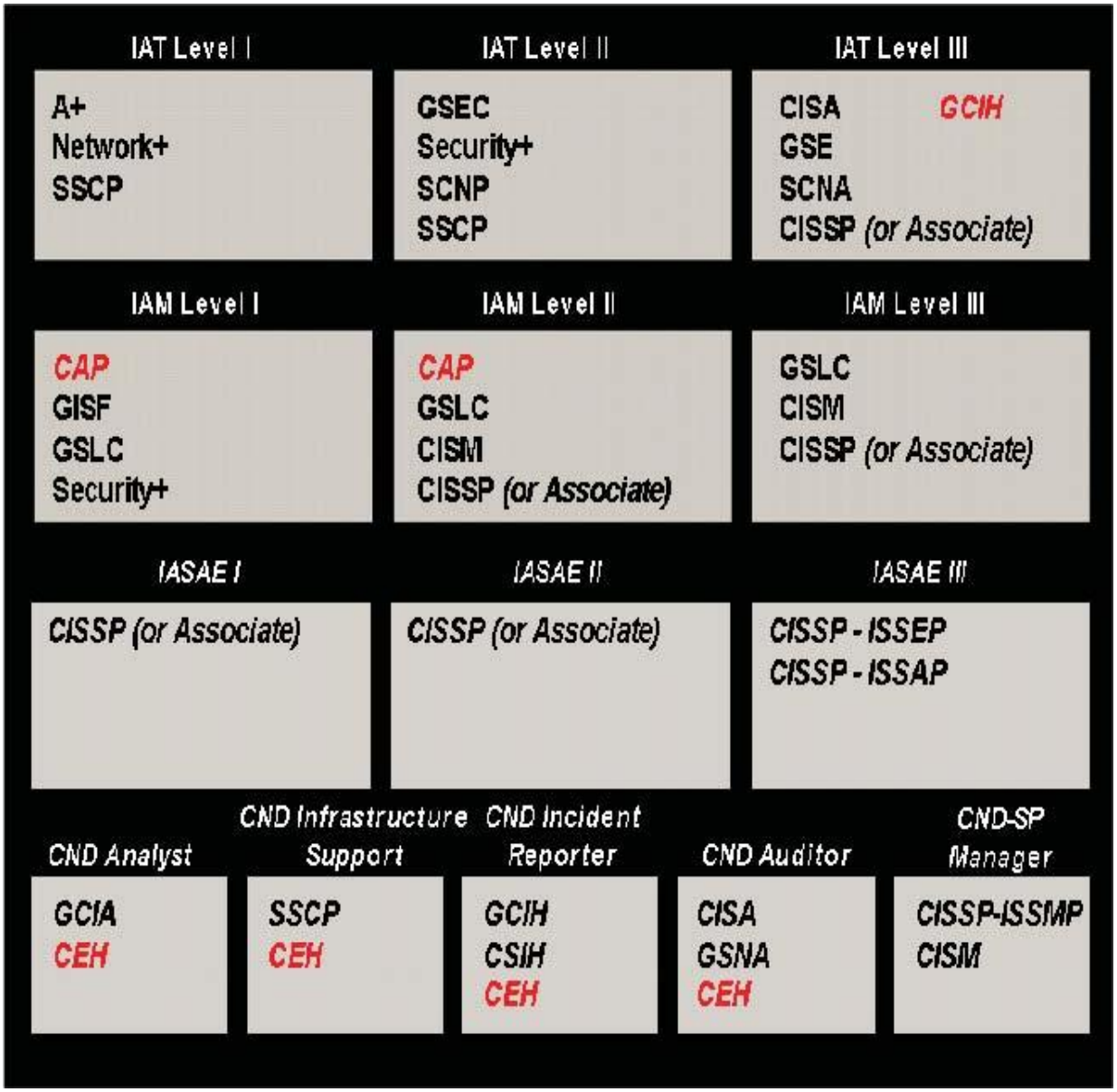

Table A-1. DoD Approved Baseline Certifications

Note: Per DoD 8570.01-M, para. C3.2.4.8.3, ACA team members who require privileged access to execute test tools or configuration checks must obtain the appropriate Computing Environment (CE) certifications for the operating systems(s) and/or security related tools/devices they support, in addition to the baseline IA certification requirement for their level.

1b. Examples of Technical Certifications

(Highly Recommended, exhibits team competency and breadth of experience)	
COMPTIA A+	JNCIE (Juniper Networks Certified Internet Expert)
Adobe Certifications	MCAD (Microsoft Certified Application Developer)
AWP (Associate Webmaster Professional)	MCP (Microsoft Certified Professional)
BEA Certified Developer	MCP+SB (MCP + Site Building)
CCA (Citrix Certified Administrator)	MCSA (Microsoft Certified Systems Administrator)
CCAE (Check Point Certified Addressing Expert)	MCT (Microsoft Certified Trainer)
CCDP (Cisco Certified Design Professional) or CCNP (Cisco Certified Network Professional)	COMPTIA Network+
CCEA (Citrix Certified Enterprise Administrator)	PMP (Project Management Professional)
CCIE (Cisco Certified Internetworking Expert)	SCJD (Sun Certified Developer for the Java 2 Platform)
Cisco Content Networking Specialist	SCNA (Security Certified Network Associate)
CIW (Certified Internet Webmaster)	Server+
CLS (Certified Lotus Specialist)	Sun Certified Developer for the Java 2 Platform
Dell Certified Enterprise Engineer	Sybase Certifications
IBM Certification	TWC900 &TWC950 (Technical Writer Certification)
Java Certifications	WOW (World Organization of Webmasters)

Table A-2. Examples of Technical Certifications

2. Support Personnel Information Worksheet

IA Work Force					
Employee Name	Gov. Civilian, Military, Contractor	IA Certification and Date	Years of IA Experience	Primary Duty/Skill Set (networks, software, pen testing, web, etc.)	Security Clearance, Investigation Type and Date

Table A-3. Support Personnel Information Worksheet

3. Annual Reporting and Re-licensing

3a. Personnel Recertification Document Worksheet

Annual Re-Certification					
Employee Name	Gov. Civilian Military Contractor	IA Certification and Date	Primary Duty/Skill Set (networks, software, penetration testing, web, etc.)	Security Clearance, Investigation Type and Date	Annual IA Training Min 2 days IA/IT course

Table A-4. Annual Re-Certification Worksheet

3b. ACA Recertification Memo

The memo must document any changes that have occurred from the original ACA application as well as document the review and results of the following items from the application: 11, 11a, through 11d, and signed by the ACA Lead.

Appendix B -Abbreviations and Acronyms

AF	Air Force
AF-CA	Air Force Certifying Authority
AF DAA	Air Force Designated Accrediting Authority
AF-GIG	Air Force-provisioned portion of the Global Information Grid
AF SIAO	Air Force Senior Information Assurance Officer
ACA	Agent of the Certifying Authority
C&A	Certification and Accreditation
CAP	Certification and Accreditation Professional
CE	Computing Environment
CEH	Certified Ethical Hacker
CISA	Certified Information Security Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information System Security Professional
CND	Computer Network Defense
CND-SP	Computer Network Defense Service Provider
CSIH	Computer Security Incident Handler
DAA	Designated Accrediting Authority
DIACAP	Department of Defense (DoD) Information Assurance Certification and Accreditation Process
DIP	DIACAP Implementation Plan
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
GCIA	GIAC Certified Intrusion Analyst

GCIH	GIAC Certified Incident Handler
GIAC	Global Information Assurance Certification
GISF G	IAC Information Security Fundamentals
GSE	GIAC Security Expert
GSEC	GIAC Security Essentials Certification
GSLC	GIAC Security Leadership Certificate
GSNA	GIAC Systems and Network Auditor
IA	Information Assurance
IAM	Information Assurance Manager
IASAE	Information Assurance System Architect and Engineer
IAT	Information Assurance Technician
IAW	In Accordance With
$(ISC)^2$	International Information Systems Security Certification Consortium
ISO	Information System Owner
ISSEP	Information System Security Engineering Professional
ISSMP	Information Systems Security Management Professional
KS	Knowledge Service
MOA	Memorandum of Agreement
PIT	Platform Information Technology
PSA	Project/Program Support Agreement
PM	Program Manager
RDT&E	Research, Development, Test and Evaluation
SCNA	Security Certified Network Architect
SCNP	Security Certified Network Professional
SIP	System Identification Profile
SLA	Service Level Agreement
SSCP	System Security Certified Practitioner

SOW	Statement of Work
STIG	Security Technical Implementation Guide
U.S.	United States

Appendix C – Memorandum of Agreement (MOA) Template

MEMORANDUM OF AGREEMENT (MOA)

Version 4.0

Agent of the Certifying Authority (ACA) <<Special (if required)>> License

BETWEEN

Air Force Certifying Authority (AF-CA)

AND

<<ACA Requesting Individual/Organization>>

References: (a) AFI 33-210, "Air Force Certification and Accreditation (C&A) Program (AFCAP)" December 23, 2008

(b) AFCAP Agent of the Certifying Authority (ACA) Licensing Guide"
<<date of current guide>>

This MOA establishes compliance with the AF Certification and Accreditation (C&A) Program (AFCAP) ACA <<Special (if requested)>> License. This ACA MOA is between the Air Force Certifying Authority (AF-CA) and the <<ACA individual/organization>> for the purpose of establishing the requirements and responsibilities for fulfilling the ACA role. The ACA will perform activities on behalf of the AF-CA while maintaining the highest levels of personal and professional ethics.

1. <<ACA individual/organization will enter here a very high level justification why an ACA License is required or if a Special ACA License is required. If a Special ACA License is requested, define here the IS category, community, or grouping (i.e. Medical, RDT&E, PIT, .edu, etc.).>>

1.1. << Full Name>> is the designated ACA Lead.

1.2. << Full Name>>is the designated ACA Assistant Lead.

2. <<ACA individual/organization>>Requirements and Responsibilities:

2.1. Ensure all business rules and requirements are maintained as prescribed in AFI 41 33-210 and the AFCAP ACA Licensing Guide.

2.2. Ensure validation remains completely independent and separate from any system-related personnel pressure or influences from outside of the ACA 44 organization.

2.3. Ensure availability of ACA services for all Information Systems (IS), and ensure all IS and organizations receive same level of evaluation and customer support.

2.4. Provide meeting inputs as part of a system's DoD Information Assurance C&A Process (DIACAP) Team representing the AF-CA throughout the system lifecycle, and participate as a non-voting IA member of the AFCAP Technical Advisory Group.

2.5. Ensure sufficiently skilled personnel resources (with prescribed level of experience, as required in DoDD 8570.1) are utilized to perform expected workload.

2.6. Ensure all required and formally agreed to deliverables are met as prescribed in the AFCAP ACA Licensing Guide.

2.7. Provide the AF-CA ACA Program Manager (ACA PM) with all system documentation when and as requested in writing.

2.7.1. All documentation prepared in support of and/or resulting from ACA validation activities are the property of the government and may not be considered proprietary, in accordance with the Federal Acquisition Regulation 59 (FAR) Part 27.

2.7.2. All agreements and contracts with ACAs will be written in such a manner as to ensure all documentation shall be made available to the government.

2.8. ACA Lead will notify the ACA PM of any status change in the ACA Lead position, or any circumstances or potential situations impacting the ACA's ability to perform necessary technical or administrative ACA functions. The ACA PM will work with the AF-CA, ACA Lead, and/or the program office to address the situation.

2.9. To avoid duplication of effort, the ACA will pre-coordinate with ACA PM prior to initiating validation of any system/version. The ACA will provide the ACA PM with and maintain a current list of systems the ACA has agreed to validate. The template is available from ACA PM.

2.10. ACA organization will enter into a documented system validation agreement (i.e. MOA, Service Level Agreement, Project/Program Support Agreement, etc.) with the system PM before validation starts. The agreement will include, but not be limited to, the specifics listed in the AFCAP ACA Licensing Guide and will be signed by the system PM and ACA Lead.

2.11. The ACA Lead and their selected personnel will attend meetings and teleconferences scheduled by the ACA PM. These meetings and teleconferences will be held to discuss validation issues that may affect how system IA controls are validated (including validation criteria for specific IA controls), and to ensure continuity between all ACAs. These meetings are an opportunity to work issues at the lowest possible level.

2.12. The ACA Lead may request a meeting or teleconference with the ACA PM to discuss problems, issues, process change requests, quality, trends, and upcoming ACA or ACA Program changes.

2.13. The ACA Lead will work issues directly with the system PM. If the issue becomes an impassable situation, the ACA Lead will contact the ACA PM for resolution.

2.14. The ACA Lead will provide the ACA PM with on-time documentation as requested in writing. All documentation resulting from ACA validation activities are the property of the government and may not be considered proprietary. All agreements and contracts with ACAs will be written in such a manner as to ensure all documentation shall be made available to the government.

2.15. The ACA Lead will provide all certification determination recommendations, residual risk assessments, validation results, etc. to the AF-CA in the format prescribed by the AF-CA and/or AF DAA. Any/all issues/deficiencies will be returned to and resolved by the ACA Lead.

2.16. The ACA Lead can send an MOA change request to the ACA PM.

3. ACA PM Requirements and Responsibilities:

3.1. Provide the ACA with the ACA Licensing Guide, licensing request package templates, and assistance as required.

3.2. Update the ACA Lead with any/all changes to validation procedures, documentation requirements, or AF-CA/AF DAA processes in an “ACA System Program Update” email at least monthly.

3.3. Conduct meetings or teleconferences with the ACA Lead or Assistant ACA Lead to discuss any ACA issues on as needed basis.

3.4. Elevate problems, issues, or situations that cannot be resolved with the ACA Lead through the AF-CA or AF SIAO as required.

3.5. Send MOA change requests to AF-CA for approval.

4. AF-CA Requirements and Responsibilities:

4.1. Review all ACA licensing requests and either approve licensing requests or recommend disapproval to the AF SIAO.

4.2. Conduct teleconferences with the ACA Lead to discuss overall ACA efforts, quality, problems, situations, trends, and other issues as needed. Elevate unresolved issues to the AF SIAO as required.

4.3. Monitor ACA performance and recommend to the AF SIAO revocation of the ACA license if the ACA repeated does not follow the AFCAP ACA Licensing Guide, ACA PM Guidance, or AF-CA Guidance.

4.4. Issue the final certification determination.

_____
<<ACA Lead>>
<<Signature Block>>

_____
<<AF-CA>>
<<Signature Block>>
Air Force Certifying Authority (AF-CA)