

**BY ORDER OF THE COMMANDER  
673D AIR BASE WING (PACAF)**



**AIR FORCE INSTRUCTION 31-501**

**673D AIR BASE WING  
Supplement**

**4 DECEMBER 2013**

**Security**

**PERSONNEL SECURITY PROGRAM  
MANAGEMENT**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

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

**RELEASABILITY:** There are no release restrictions on this publication

---

OPR: 673 ABW/IPO

Certified by: 673 ABW/CD  
(Mr. Donald C. Weckhorst)

Supersedes: AFI 31-501/3WG Sup 1,  
29 June 2007

Pages: 17

---

This supplement implements and extends the guidance of Air Force Instruction (AFI) 31-501, *Personnel Security Program Management*, **27 January 2005**, and applies to all host, tenant, associate (participants), and temporary (TDY) organizations on Joint Base Elmendorf-Richardson (JBER). This supplement applies to Air National Guard and Air Force Reserve units on the installation that fall under Air Force program oversight. This supplement provides a baseline requirement for managing the Personnel Security Program. The office of primary responsibility (OPR) has determined that there will be no waivers granted for any part of this publication and it may not be supplemented. Refer recommended changes and questions about this publication to the OPR using the AF Form 847, *Recommendation for Change of Publication*. Route the AF Forms 847 through the appropriate chain of command. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). See **Attachment 1** for Glossary of References and Supporting Information. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

**SUMMARY OF CHANGES**

**This document has been substantially revised and must be completely reviewed.** It's rewritten to better align host wing supplement with the current AFI and PACAF Supplement. It

provides a significant rewrite and clarification of Activity Security Manager (ASM) functions at the unit level. All US Army affiliated personnel should contact the Installation Security Intelligence Office at 384-3955 for specific guidance on all matters contained herein as significant procedural differences exist.

**2.4. Types and Scope of Personnel Security Investigations.** Electronic Questionnaire for Investigation Processing by Design (e-QIP) replaces Electronic Personnel Security Questionnaire (EPSQ) as used throughout the basic AFI.

2.4.3. Minimum Background Investigation (MBI) are required on all civilian/contract employees assigned to **public trust** (moderate risk) positions. Background Investigation (BI) are required on all civilian/contract employees assigned to public trust (high risk) positions.

2.4.4. National Agency Check Plus Written Inquiries (NACI) is now the baseline background investigation required for all civilian/contractor/volunteer personnel assigned to **non-sensitive** (low risk) positions or requiring a Common Access Card (CAC) to access Federal facilities, access to restricted areas that don't contain classified information or unclassified information systems on a permanent basis. All Air Force positions that previously required the initiation or completion of a National Agency Check (NAC) now require a NACI or higher investigation.

2.4.5. Access National Agency Check with Written Inquiries and Credit Check (ANACI) is required for all civilian employees assigned to non-critical sensitive positions. National Agency Check, Local Agency Check and Credit Check (NACLCLC), and NACI are not sufficient in scope for personnel assigned to these positions. **EXCEPTION:** Single Scope Background Investigations (SSBI) are sufficient in scope for civilians assigned to non-critical sensitive positions, provided there has been no break in service greater than 24-months.

2.4.6. National Agency Check, Local Agency Checks and Credit Check (NACLCLC). NACLCLCs are required for military and contractor personnel who need access to Secret information. **NOTE:** Company Facility Security Officers (FSO) will submit contractors assigned to National Security positions for appropriate Personnel Security Investigation (PSI).

2.4.8. Periodic Reinvestigation (PR). PRs are investigations conducted at prescribed intervals for the purpose of updating a previously completed background investigation. **NOTE:** Because of significantly improved security clearance investigative/adjudication timelines, effective 24 August 2011, all PRs will not be submitted earlier than 60 days of the anniversary date of the subject's current investigation.

2.4.10. **(Added)** . Special Agreement Check (SAC) is a finger print check that is required with all initial investigations. The 673 ABW Information Protection Office (IPO) can provide ASM, and Trusted Agents (TA) the advanced finger print results for CAC card issuance in accordance with HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*. **NOTE:** OFI Form 86C, *Special Agreement Checks*, are required for members who have a top secret clearance and marry or cohabitate with a Foreign National. In this case, ASMs must notify IPO as soon as possible for guidance.

3.1. Authority to Designate Sensitive Positions. Commanders and Human Resources Specialist will use the Office of Personnel Management (OPM) position designation tool at <http://www.opm.gov/investigate/resources/position/index.aspx> to aid in position designation. All position designations must be updated in the Defense Civilian Personnel Data System (DCPDS).

3.2. Within JBER, IPO submits all PSI requests. **EXCEPTION:** Civilian Personnel Flight and Non-Appropriated Funds Human Resource Office are authorized requesters and submit all PSIs for new hires. Contractors assigned to National Security positions will have their PSIs submitted by the company FSOs.

3.2.1. Suitability determinations (no determination made (NDM)) that are returned from the Consolidated Adjudication Facility (CAF) will be made accordingly:

3.2.1.1. **(Added)** . IPO sends the case file, NDM memorandum, and OPM Form 79A, *Report of Adjudicative Action*, to the unit Commander and appropriate Human Resource Office (Civilian Personnel Flight (CPF)/ Non-Appropriated Funds (NAF)/Contracting) for action.

3.2.1.2. **(Added)** . The CPF/NAF Human Resources ((HR) Office):

3.2.1.2.1. **(Added)** . Determines if the individual is deemed suitable for employment in accordance with 5 CFR 731.201-202, *Suitability Determinations*. Coordination/consultation with the supervisor and or commander may be made.

3.2.1.2.2. **(Added)** . If employee is determined **suitable**, CPF/NAF signs off on the OPM Certificate of Investigation and the form is filed in the individual's Official Personnel Folder (OPF) in accordance with AFI 36-114, *Guide to Personnel Recordkeeping*.

3.2.1.2.3. **(Added)** . If applicant is determined **unsuitable**, CPF/NAF fills out the OPM Form 79A, and coordinates with the employee's supervisor and or commander. CPF/NAF forwards the OPM Form 79A to OPM. **NOTE:** For contractors, the unit Commander will coordinate appropriate actions with the Contracting office, ASM, and unit Quality Assurance representative.

3.2.3.4. **(Added)** . The ASM will be required to update the Joint Verification System (JVS) with the suitability determination via the Information Technology (IT), Public Trust or Child Care links.

3.6. The Civilian Personnel Flight ensures a pre-employment waiver is completed by commanders on all new employees who are designated to fill Non-Critical Sensitive, Critical Sensitive or Special Sensitive positions, prior to the individual reporting for work. The individual's unit of assignment will provide a copy of the pre-employment waiver letter to IPO. A pre-employment waiver does not authorize the individual access to classified information, IT systems, a common access card or a restricted area badge. The individual must have a security clearance for access to classified information or a favorable investigation for access to IT systems or unescorted entry to restricted areas.

3.10. Security Clearance Authority. The Department of Defense (DoD) CAF is the designated authority to grant, suspend, deny or revoke personnel security clearances and SCI access.

3.10.1. The CAF issues security clearance eligibility based on the type of investigation conducted. Commanders grant access to classified information based on the level of position occupied by the individual. Access must be reflected in Joint Verification System (JVS). If a member's security clearance goes "out of scope" the commander must submit a Continuous Access letter to IPO in order for member to maintain access to classified information pending submission of periodic reinvestigation to OPM (see **Attachment 2**, this supplement).

3.11. **Interim Security Clearances.** ASMs will coordinate interim clearances with IPO prior to the commander granting an interim clearance. IPO will ensure all interim security clearance requirements have been met and any potentially derogatory information is identified for the

commander's review. IPO may make recommendations to the subject's commander concerning eligibility. The subject's commander will determine what is considered to be "favorable" when determining whether to grant an interim security clearance. Commanders may grant interim security clearances, through IPO, for Top Secret and Secret access to classified information when the requirements within AFI 31-501, paragraph 3.11 have been met. Interim clearances may be revoked at any time based on unfavorable information identified in the course of the investigation. Interim clearances should be held to mission essential personnel only and strict scrutiny should be used in granting interim clearances.

3.11.1. Interim **Top Secret (TS)** clearances must be based on all of the following:

3.11.1.1. IPO must verify a favorable NACI, NACLIC, or ANACI has been completed. The investigation is acceptable if there is no break in service over 24 months.

3.11.1.2. Unit commander or staff agency chief must conduct a review of the subject's Personnel Security Questionnaire (PSQ). Commanders must sign block 26 of the AF Form 2583, *Request for Personnel Security Action*, and annotate in the remarks section, "I have reviewed subject's PSQ and would like to grant an interim TS."

3.11.1.3. ASM accomplishes the AF Form 2583 requesting local files checks of personnel records including military personnel information file (PIF) and civilian official personnel file (OPF), Security Forces, medical records (Public Health), and other security records as appropriate. The AF Form 2583 is valid for up to 90 days after the last signature.

3.11.1.4. IPO must receive a confirmed receipt of a SSBI request submitted to OPM.

3.11.1.5. ASM submits package to IPO: AF Form 2583 (with all signatures) and a copy of subject's PSQ for JVS update. Once JVS is updated, IPO will notify ASM.

3.11.4. Interim **Secret** clearances must be based on all of the following:

3.11.4.1. Same procedures as for an Interim TS, except IPO must confirm subject has an "open" investigation (NACLIC or ANACI) on file with OPM.

3.11.6. For Civilians:

3.11.6.1. Former military members with a break in service of 24 months or less and SSBI within five years do not have to resubmit an SSBI for critical sensitive positions. Periodic Reinvestigations will be submitted for SSBI over five years old. SSBI over seven years, will require an initial SSBI instead of a periodic reinvestigation. Former military members and current reserve and guard personnel occupying noncritical sensitive positions must submit an Access National Agency Check Plus Written Inquiries and Credit Check (ANACI).

3.11.6.2. Same procedures as for Interim TS and Secret, except ASMs must add pre-employment waiver memorandum to the interim clearance package.

3.15. **One Time Access.** Document one time access by using AF Form 2583. Approving authorities sign Item 26 when granting access. The ASM will maintain the AF Form 2583 until the access is no longer needed. Complete an AF Form 2587, *Security Termination Statement*, when access is terminated. Document actions in JVS, when applicable.

3.24.1. The NACI is the minimum investigative requirement for access to restricted areas and IT systems not involving access to classified information.

3.24.8. Interim access to restricted areas may be granted to military, civilians, and contractors. Use the same procedures for interim access as established in paragraph 3.11, of this instruction.

3.24.10. IPO submits the applicable background investigation to OPM for contractor personnel requiring unescorted entry to restricted areas that don't contain classified information. This only applies to contractors who do not require access to classified information.

3.27.3. Commanders may recommend to the JBER Communications and Information Systems Officer (CSO) that interim IT system access be granted. The CSO (673 CS/CC) may waive on a case by case basis the investigative requirements for access to IT systems pending completion of a favorable NACI, MBI, BI, NACLAC ANACI, or SSBI after favorable review of the completed personnel security questionnaire for the investigation. The CSO and the Unit Information Assurance Officer (IAO) will confirm all interim IT system access requirements are met prior to access.

3.27.3.7.2. IPO submits the applicable background investigations to OPM for contractor personnel requiring access to unclassified IT systems. This only applies to contractors who do not require access to classified information.

3.28. **Periodic Reinvestigations (PR).** PRs are required every five years for Top Secret and ten years for Secret. The IPO are the designated authorized requester and submits all requests for reinvestigations to OPM. The earliest IPO can submit a reinvestigation is 60 days from the subject's last close date.

3.30. **(Added) . Contractor Suitability Determinations.** Unit commanders will make suitability determinations for contractors assigned to their unit who require a favorable background investigation for contract performance. The unit is responsible for forwarding the decision to OPM (via OPM Form 79A Report of Adjudicative Action form).

4.1. **Prior Federal Civilian Investigations.** Investigations previously conducted on civilian employees are suitable and accepted for granting immediate access to classified information as long as they are the same position sensitivity, not out of scope and the subject has not had a single break in service more than 24 months.

4.1.1.3. CPF and Non-Appropriated Funds (NAF) human resource office confirms with OPM that a valid investigation is on file and notifies the CAF. HR can send a message or call CAF customer service to request CAF order the investigation.

5.1.1. ASMs must maintain an OPM Portal/e-QIP account and JVS account in order to manage the Personnel Security Program for their organization.

5.1.1.1. ASMs will produce a JVS personnel roster by the 10th of each month. The ASM will verify all the information on the roster is correct and take actions to correct any discrepancies such as indoctrinations, non-disclosure agreement (NDA), position sensitivity, and personnel assigned.

5.1.1.2. **(Added) .** ASMs will produce a JVS PR report by the 10th of each month and notify unit members within **three** duty days that they are due for a PR. ASMs will develop a tracking system of individual's notified to complete their e-QIP. ASMs will provide IPO with a copy of the PR report with all annotations listed. ASMs will notify the commander and supervisor of individuals who fail to meet their established suspense and initiate a Security Information File if applicable.

5.4. **Request Procedures.** The following are investigation request procedures

5.4.1. **(Added)** . ASMs determine what type of investigation to initiate based on the unit's monthly PR report or other applicable documents (mandatory top secret AFSC, assignment Records on Individual Persons (RIP), position code on Unit Manning Document (UMD) and checking JVS. **NOTE:** If subject will retire/separate within 12 months, do not initiate an e-QIP request, call IPO for guidance.

5.4.2. **(Added)** . ASMs must conduct a Local File Check (LFC) using the AF Form 2583. Use the LFC and ASM e-QIP checklist located on the 673 ABW/IPO SharePoint ® site located at <https://jber.eim.elmendorf.af.mil/673ABW/IPO/Personnel%20Security/Forms/AllItems.aspx?RootFolder=%2f673ABW%2fIPO%2fPersonnel%20Security%2fEQIP%20Aids%20and%20Tools%20for%20USMs&FolderCTID=&View=%7b6F282E4B%2dDF62%2d4A7F%2dB4D7%2d16EC587CE0CA%7d> to ensure proper e-QIP initiation.

5.4.3. **(Added)** . ASM will log into the OPM portal and link to the e-QIP agency <https://opmis.xsp.org/member/index.cfm> and create an e-QIP initiation request for subject.

5.4.4. **(Added)** . ASM will notify subject via e-mail or in person of the initiation. ASM will establish a deadline of 15 days or less and ensure subject understands how to access his/her e-QIP account and complete his/her questionnaire. If subject breaks the ASM suspense, the ASM will brief unit Commander and take action as appropriate. **NOTE:** Failure to complete security paperwork is grounds for Security Information File (SIF) establishment in accordance with the Department of Defense (DoD) adjudicative guideline Personal Conduct and AFI 31-501.

5.4.5. **(Added)** . Once subject submits their e-QIP for review, the ASM must conduct a quality review of the e-QIP. If the e-QIP is filled out completely, the ASM will submit the e-QIP to IPO for review/approval. If the form needs corrections, the ASM will reject the form back to subject and notify subject of corrections needed.

5.4.6. **(Added)** . Once the ASM releases e-QIP to IPO, at that time the ASM must send the AF Form 2583, ASM e-QIP checklist and any other applicable documents (assignment RIP, orders, and so forth) to IPO. **NOTE:** The AF Form 2583 is only valid for 90 days from the last date it was signed. IPO will not review/approve an e-QIP unless we have the documents stated above.

5.4.7. **(Added)** . IPO will review the e-QIP; if errors are found, it will be sent back to the subject for corrections, if error free, the subject will be notified to schedule an appointment for finger-printing and to sign the release forms, if applicable.

5.4.8. **(Added)** . Once IPO submits the e-QIP to OPM, IPO will update the Personnel Security Questionnaire (PSQ) sent date in JVS and annotate submission on the hard copy of AF Form 2583. The AF Form 2583 will be placed in the ASMs box. ASMs must use the AF Form 2583 as a tracking tool and check JVS within 7-10 days to ensure subjects investigation has opened. If not, ASMs must contact IPO. ASMs must periodically check JVS to ensure subject's investigation closes and gets adjudicated. If an investigation is open longer than 120 days or pending adjudication longer than 60 days, the ASM must contact IPO for further guidance.

5.4.9. **(Added)** . ASMs will not sign off on *Outbound Assignment Memorandums for permanent change of station (PCS)*, unless subject's investigation meets the PCS requirements or the new investigation has been submitted (left the base) to OPM. If unsure, contact IPO for

guidance. Unit members are not allowed to receive PCS orders until investigation requirements have been met in accordance with the members assignment RIP.

7.1.2. All unit commanders will review the security access requirement/position coding (SAR/PC) codes **by 15 February every year** for accuracy and document the results in a memorandum (see **Attachment 3**, this supplement) and supply IPO with copy. All authorization change requests (ACR) for SAR codes must be routed through IPO, Civilian Personnel, and 11AF/CC, if applicable. Any changes to civilian positions require the unit to follow-up with the civilian personnel office to ensure the position sensitivity gets updated on the subject's Position Description (PD) and updated in the Civilian Personnel Data System. The unit is responsible for all routing of SAR code change requests. An example SAR code change request memorandum is listed in **Attachments 4 and 5**, this supplement.

**7.5. Investigative Requirements for Air Force Deployments, Operational or Contractual Exigencies.** Home station commanders will coordinate this action with deployed commanders before granting interim Top Secret access. Document interim Top Secret access by using the AF Form 2583. Commanders sign Item 26 when granting interim access. The deployed member will maintain the original AF Form 2583 for use at the deployed location and the home station ASM will maintain a copy of the AF Form 2583. Access will be discontinued upon return to home station by executing an AF Form 2587, *Security Termination Statement*. **NOTE:** If deployed location will not accept and interim or SCI access is required, the subject must be submitted for a SSBI.

7.9. The Joint Personnel Adjudication System (JPAS) is now called the JVS.

7.9.5.5. ASMs that have a secret clearance and have completed the JVS training ([www.dss.mil](http://www.dss.mil)) in order to be given level 6 access. ASMs will "service" all unit members into their Security Management Office (SMO). ASMs will "service" contractors assigned to integrated visitor groups supporting their unit. ASMs will manage JVS within their unit by performing the following actions: In/out process members, indoctrinate/debrief unit members (assign/remove access level), execute and update SF 312, *Non-Disclosure Agreement*, if applicable, send/manage visit notifications, monitor system notifications, maintain a personnel and PR report within the last 30 days. **NOTE:** Debrief members within 5 duty days of permanent change of stations, separation or retirement.

7.12.1. IPO, Civilian Personnel and Non-Appropriated fund HRs, identified by IPO letter, are authorized callers to the DoD CAF.

8.2.1.4.1. **(Added)** . If access is suspended, an AF Form 2587 must be accomplished and included in the Security Information File (SIF).

8.2.1.7. Once all pertinent information is obtained to close a SIF, the commander will request closure of the SIF in writing to the CAF through the IPO within 120 days of SIF establishment. Memorandum will include a recommendation whether to grant, reinstate, deny, or revoke subject's security clearance. If more time is needed, a SIF extension request memorandum must be submitted to the CAF through IPO prior to the 120 day deadline.

8.2.2.1. ASMs provide guidance to commanders on SIF establishment. IPO is the OPR for Top Secret and Secret security clearance SIFs; SSO is OPR for SCI access SIFs.

8.2.2.1.1. **(Added)** . When IPO becomes aware of potentially derogatory information, IPO will notify the unit Commander via ASM to consider a SIF establishment. If the individual is SCI-indoctrinated, the IPO will notify the servicing Special Security Office (SSO), who will in turn notify subject's commander.

8.2.3.1. **(Added)** . Unit Commanders, First Sergeants, and Staff Agency Chiefs must confer with ASMs when derogative information arises and falls within the guidelines set forth in AFI 31-501, paragraph, **8.2.1.3.1**, and DoD 5200.2-R, *Department of Defense Personnel Security Program*, Chapter 2, paragraph **2-200**.

8.2.3.2. **(Added)** . The ASM will provide IPO with a 60-day update in writing on the status of the SIF and all supporting documents prior to final SIF closure letter from the Commander.

8.6.3. The ASM is the point of contact (POC) at the unit level and the IPO is the POC at the Wing level.

8.7. **Security Clearance Reinstatement.** Submit requests through the IPO after 365 days from revocation/denial.

10.4. **(Added)** . **File Copy Personnel Security Questionnaires (PSQ).** File copy PSQs must remain under the control of the authorized requester (IPO). Once subjects PSQ is complete, IPO will send PSQ file copy to subject for their records and destroy file copy. ASMs will not maintain PSQ copies for unit personnel.

11.1.4.1. **(Added)** . Wing level IPO will review units' personnel security program during annual Information Protection Management Evaluation (IPME).

11.2. **(Added)** . **Information Collections.** No information collections are required by this publication.

BRIAN P. DUFFY, Colonel, USAF  
Commander

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFMAN 33-363, *Management of Records*, 1 March 2008.

DoD 5200.2-R, *Department of Defense Personnel Security Program*, January 1987.

AFI 31-501, *Personnel Security Management*, 27 January 2005.

AFI 36-114, *Guide to Personnel Recordkeeping*, 1 November 1997.

HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, 27 August 2004.

OPM INV-15, *Requesting Personnel Investigations*, 12 April 2012.

***Adopted Forms***

AF Form 847, *Recommendation for Change of Publication*.

OPM form 79A, *Report of Adjudicative Action*.

OFI Form 86C, *Special Agreement Check*.

AF Form 2583, *Request for Personnel Security Action*.

AF Form 2587, *Security Termination Statement*.

SF 312, *Non-Disclosure Agreement*.

***Abbreviations and Acronyms***

**AFSC**—Air Force Specialty Code.

**AFI**—Air Force Instruction.

**AFRIMS**—Air Force Records Information Management System.

**ANACI**—Access National Agency Check Plus Written Inquiries and Credit Check.

**ASM**—Activity Security Manager.

**BI**—Background Investigation.

**CAC**—Common Access Card.

**CAF**—Consolidated Adjudication Facility.

**CPF**—Civilian Personnel Flight.

**CSO**—Communications System Officer.

**DAA**—Designated Approving Authority.

**DCPDS**—Defense Civilian Personnel Data System.

**DoD**—Department of Defense.

**EPSQ**—Electronic Personnel Security Questionnaire.

**e-QIP**—Electronic Questionnaire for Investigation Processing.  
**FSO**—Facility Security Officer.  
**HR**—Human Resources.  
**HSPD-12**—Homeland Security Presidential Directive-12.  
**IAO**—Information Assurance Office.  
**IPO**—Information Protection Office.  
**IT**—Information Technology Systems.  
**JBER**—Joint Base Elmendorf-Richardson.  
**JPAS**—Joint Personnel Adjudication System.  
**JVS**—Joint Verification System.  
**LAN**—Local Area Network.  
**LFC**—Local File Check.  
**MBI**—Minimum Background Investigation.  
**NAC**—National Agency Check.  
**NACI**—National Agency Check with Written Inquires.  
**NACLC**—National Agency Check, Local Agency Checks, and Credit Checks.  
**NAF**—Non-Appropriated Funds.  
**NDA**—Non-Disclosure Agreement.  
**NDM**—No Determination Made.  
**OPF**—Official Personnel File.  
**OPM**—Office of Personnel Management.  
**OPR**—Office of Primary Responsibilities.  
**PCS**—Permanent Change of Station.  
**PD**—Position Description.  
**PIF**—Personnel Information File.  
**POC**—Point of Contact.  
**PR**—Periodic Review.  
**PSI**—Personnel Security Investigation.  
**PSQ**—Personnel Security Questionnaire.  
**RDS**—Records Disposition Schedule.  
**RIP**—Records on Individual Persons.  
**SAC**—Special Agreement Check.

**SAR**—Security Access Requirement.

**SAR/PC**—Security Access Requirement/Position Coding.

**SCI**—Sensitive Compartmented Information.

**SIF**—Security Information File.

**SMO**—Security Management Office.

**SSBI**—Single Scope Background Investigation.

**SSO**—Special Security Office.

**TA**—Trusted Agent.

**TDY**—Temporary Duty.

**TS**—Top Secret.

## Attachment 2

## CONTINUOUS ACCESS TO CLASSIFIED INFORMATION MEMORANDUM

## Figure A2.1. Continuous Access To Classified Information Memorandum

	DATE
MEMORANDUM FOR 673 ABW/IPO	
FROM: YOUR UNIT/CC	
SUBJECT: Continued Access to Classified Pending e-QIP submission to OPM	
<ol style="list-style-type: none"><li>1. Rank Full Name is assigned to the unit and requires continued access to classified information pending completion of e-QIP and IPO submission to the Office of Personnel Management (OPM). OR the member will separate/retire within the 12 months and no PR is required. The (Unit) mission essential functions cannot be met without continued access for Rank/Name.</li><li>2. I am not aware of any information relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information.</li><li>3. Rank/Name is unable to complete e-QIP . (provide reason).</li><li>4. How long will this access be good for? Provide date here.</li></ol>	
<b>NOTE:</b> The goal is to submit ALL personnel on time; this letter should only be used only in unusual circumstances that prevent subject from completing e-QIP and submitting to OPM prior to going "out of scope" or subject will retire/separate within 12 months.	
<ol style="list-style-type: none"><li>5. POC for this letter is ASM Name and Rank at 55X-XXXX.</li></ol>	
	NAME, RANK, USAF Commander
cc: ASM	

## Attachment 3

## SAMPLE ANNUAL SAR CODE REVIEW MEMORANDUM

Figure A3.1. Sample Annual SAR Code Review Memorandum

	DATE
MEMORANDUM FOR 673 FSS/FSMM	
FROM: (Commander/Equivalent)	
THRU: 673 ABW/IPO	
SUBJECT: Security Access Requirement (SAR) Code Annual Review	
<p>1. In accordance with AFI 31-501, paragraph 7.2 (7.2.13), I have conducted an annual review of all unit SAR/position codes. All SAR codes on the Unit Manning Document (UMD) reflect the appropriate investigative requirement for the position. No changes are needed at this time.</p> <p>2. Unit POC for this request is _____, 552-####.</p>	
CC/EQUIVALENT SIGNATURE BLOCK (Commander/Division Chief)	

Attachment 4

SAMPLE SAR CODE CHANGE REQUEST FOR CIVILIANS

Figure A4.1. Sample SAR Code Change Request for Civilians

DATE																
MEMORANDUM FOR 673 FSS/FSMM																
FROM: (Commander/Division Chief)																
THRU: 673 ABW/IP 673 FSS/FSMC 11 AF/CC (if upgrading to SAR 5 (TS))																
SUBJECT: Security Access Requirement (SAR) Code Change Request for Civilian Positions																
1. I have conducted a SAR code review of the Unit Manning Document (UMD) and request a SAR code change to the following position(s):																
<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;"><u>PAS</u></th> <th style="text-align: left;"><u>OSC</u></th> <th style="text-align: left;"><u>POSN NO</u></th> <th style="text-align: left;"><u>AFSC</u></th> <th style="text-align: left;"><u>GRADE</u></th> <th style="text-align: left;"><u>SCPD</u></th> <th style="text-align: center;"><u>CURRENT SAR CODE</u></th> <th style="text-align: center;"><u>CHANGE TO SAR CODE</u></th> </tr> </thead> <tbody> <tr> <td>XXXX</td> <td>CCQ</td> <td>002000010R</td> <td>3S071</td> <td>GS-07</td> <td>9G0014</td> <td style="text-align: center;">5</td> <td style="text-align: center;">7</td> </tr> </tbody> </table>	<u>PAS</u>	<u>OSC</u>	<u>POSN NO</u>	<u>AFSC</u>	<u>GRADE</u>	<u>SCPD</u>	<u>CURRENT SAR CODE</u>	<u>CHANGE TO SAR CODE</u>	XXXX	CCQ	002000010R	3S071	GS-07	9G0014	5	7
<u>PAS</u>	<u>OSC</u>	<u>POSN NO</u>	<u>AFSC</u>	<u>GRADE</u>	<u>SCPD</u>	<u>CURRENT SAR CODE</u>	<u>CHANGE TO SAR CODE</u>									
XXXX	CCQ	002000010R	3S071	GS-07	9G0014	5	7									
2. JUSTIFICATION. <i>*This paragraph must contain sufficient justification to warrant the action and, if previously coordinated, include HQ PACAF POC and phone number. (Do not use continuity or personnel challenges as a reason).</i> Example: The duties of position(s) no longer require access to national security information at the levels currently coded. Request the civilian position(s) identified above be downgraded from SAR code 5 (Top Secret) to SAR code 7 (Secret). OR Request the civilian position(s) identified above be downgraded from SAR code 7 (Secret) to a SAR code 8 (non-sensitive-no access to classified). Note: Be sure to provide justification for every position change requested; detailed justification required for upgrades to Top Secret.																
3. Unit POC for this request is _____, 552-####.																
CC/Equivalent SIGNATURE BLOCK (Commander/Division Chief)																

1st Ind, 673 ABW/IP

MEMORANDUM FOR 673 FSS/FSMC

Concur/Nonconcur

MARK A. MEYER, GS-13, DAF  
Chief, Information Protection

2d Ind to CC/Equivalent, x Jan 13, SAR Code Change Request

MEMORANDUM FOR 673 FSS/FSMM or 11AF/CC

Concur/Nonconcur

LINDA L. GRUE, GS-12, DAF  
Human Resource Specialist

**NOTE: IF REQUESTING A SAR CODE POSITION UPGRADE TO TOP SECRET (SAR CODE 5), THIS LETTER MUST BE ROUTED VIA STAFF SUMMARY SHEET FOR 11AF/CC SIGNATURE/APPROVAL.**

3d Ind to CC/Equivalent, x Jan 13, SAR Code Change Request

MEMORANDUM FOR 673 FSS/FSMM

Approved/Disapproved

RUSSELL J. HANDY, Lt Gen, USAF  
Commander

Attachment 5

SAMPLE SAR CODE CHANGE REQUEST MEMORANDUM FOR MILITARY

Figure A5.1. Sample SAR Code Change Request Memorandum for Military

DATE																
MEMORANDUM FOR 673 FSS/FSMM																
FROM: (Commander/Division Chief)																
THRU: 673 ABW/IP 11 AF/CC (if upgrading to SAR 5 (TS))																
SUBJECT: Security Access Requirement (SAR) Code Change Request for Military Positions																
1. I have conducted a SAR code review of the Unit Manning Document (UMD) and request a SAR code change to the following position(s):																
<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;"><u>PAS</u></th> <th style="text-align: left;"><u>OSC</u></th> <th style="text-align: left;"><u>POSN NO</u></th> <th style="text-align: left;"><u>AFSC</u></th> <th style="text-align: left;"><u>GRADE</u></th> <th style="text-align: left;"><u>SCPD</u></th> <th style="text-align: center;"><u>CURRENT SAR CODE</u></th> <th style="text-align: center;"><u>CHANGE TO SAR CODE</u></th> </tr> </thead> <tbody> <tr> <td>XXXX</td> <td>CCQ</td> <td>002000010R</td> <td>3S071</td> <td>GS-07</td> <td>9G0014</td> <td style="text-align: center;">5</td> <td style="text-align: center;">6</td> </tr> </tbody> </table>	<u>PAS</u>	<u>OSC</u>	<u>POSN NO</u>	<u>AFSC</u>	<u>GRADE</u>	<u>SCPD</u>	<u>CURRENT SAR CODE</u>	<u>CHANGE TO SAR CODE</u>	XXXX	CCQ	002000010R	3S071	GS-07	9G0014	5	6
<u>PAS</u>	<u>OSC</u>	<u>POSN NO</u>	<u>AFSC</u>	<u>GRADE</u>	<u>SCPD</u>	<u>CURRENT SAR CODE</u>	<u>CHANGE TO SAR CODE</u>									
XXXX	CCQ	002000010R	3S071	GS-07	9G0014	5	6									
2. JUSTIFICATION. <i>*This paragraph must contain sufficient justification to warrant the action and, if previously coordinated, include HQ PACAF POC and phone number. (Do not use continuity or personnel challenges as a reason).</i> Example: The duties of this position no longer require access to national security information at the Top Secret level. Request the military position be downgraded from SAR code 5 (Top Secret) to a SAR code 6 (Secret). Note: Be sure to provide justification for every position change requested; detailed justification required for upgrades to Top Secret.																
3. Unit POC for this request is _____, 552-####.																
CC/Equivalent SIGNATURE BLOCK (Commander/Division Chief)																

1st Ind, 673 ABW/IP

MEMORANDUM FOR 673 FSS/FSMM or 11AF/CC

Concur/Nonconcur

MARK A. MEYER, GS-13, DAF  
Chief, Information Protection

**NOTE: IF REQUESTING A SAR CODE POSITION UPGRADE TO TOP SECRET SAR CODE 5), THIS LETTER MUST BE ROUTED VIA STAFF SUMMARY SHEET FOR 11AF/CC SIGNATURE/APPROVAL.**

2d Ind to CC/Equivalent, x Jan 13, SAR Code Change Request

MEMORANDUM FOR 673 FSS/FSMM

Approved/Disapproved

RUSSELL J. HANDY, Lt Gen, USAF  
Commander