NATIONAL GUARD BUREAU
111 SOUTH GEORGE MASON DRIVE
ARLINGTON VA 22204-1373

ARNG-OIZ

19 December 2017

MEMORANDUM FOR State and Territory ARNG G-2s, G-6s and Security Managers

SUBJECT: Army National Guard (ARNG) Department of the Army Cryptographic Access Program (DACAP) Policy

1. References:

a. DoDD 5205.08, Access to Classified Cryptographic Information, 8 November 2007.

b. AR 380-40, Policy for Safeguarding and Controlling Communications Security (COMSEC) Material, 9 July 2012 with rapid action review (RAR) date 24 April 2013.

c. AR 380-67, Personnel Security Program, 24 January 2014.

d. AR 25-400-2, The Army Records Management System (ARIMS), 2 October 2007.

e. AR 25-2, Information Assurance, 23 March 2009.

f. Army National Guard (ARNG) Department of the Army Cryptographic Access Program (DACAP) Policy, 11 April 2016.

2. Applicability: This memorandum applies to all Army National Guard military and civilian personnel, contractors and consultants officially assigned to duties that require continuing access to U.S. classified cryptographic and COMSEC information. Individuals enrolled in DACAP will be subjected to random counterintelligence scope polygraph (CSP) examinations and must attend such examinations when properly notified.

3. Purpose: To provide the policy and procedures to successfully manage DACAP using existing lines of authority within the security management hierarchy.

4. Policy: State Security Mangers (SSMs) or G-2 will manage DACAP in accordance with (IAW) AR 380-40, chapter 7, and will ensure each unit's security manager or DACAP point of contact successfully administers the program.

5. Procedures: The DACAP Program requires SSMs, G-2s, Brigade or unit security managers to develop procedures that support security clearance verification,

cryptographic access/termination certification, and requests for CSPs. These procedures include:

a. Cryptographic access/termination certification. All access certification and termination briefings for cryptographic is completed IAW AR 380-40, para 7-4.

(1) Granting Cryptographic Access:

(a) The unit commander is responsible for identifying those personnel requiring cryptographic access.

(b) Any individual who refused to sign Secretary of Defense (SD) Form 572, section I will be denied access to all classified cryptographic information.

(c) The cryptographic access certification briefing and the authorization portion of SD Form 572, Cryptographic Access Certification and Termination, is completed by the Security Manager. The access certification briefing is provided in AR 380-40, Appendix D, and is included in the memorandum format as enclosed. This briefing is read verbatim to individuals prior to receiving cryptographic access. The Security Manager, IAW AR 25-400-2, **will retain the SD Form 572 and the access briefing** for later retrieval when they are required to complete the termination certification briefing.

(d) A copy of the completed SD Form 572 and a copy of the access certification briefing is filed by the SSM for documenting DACAP enrollments. Brigade or unit security managers will provide copies of the completed SD Form 572 to the SSM. **COMEC accounts will not have any copies of a completed SD Form 572 in the COMSEC account.**

(e) The SSM, G-2, Brigade or unit security manager will provide the COMSEC Account Manager a signed memorandum of individuals submitted for enrollment into DACAP. The COMSEC Manager will verify that personnel enrolled in DACAP meet the requirements identified in AR 380-40, para 7-2. The COMSEC Manager will retain a copy of the enrollment memo on file for audit or inspection purpose. Additionally, the SSM will provide a copy of the DACAP enrollment spreadsheet to the ARNG G2 COMSEC Program Manager **no later than (NLT) 1 June** of each year.

(2) Terminating Cryptographic Access.

(a) The Brigade or unit Security Manager will complete the cryptographic termination certification briefing and the termination portion of the SD Form 572.

(b) The Brigade or unit Security Manager will provide a copy of the completed SD Form 572 and termination certification briefing to the SSM. Assigned personnel will remain enrolled in the program and subject to CSPs until terminated and debriefed IAW established guidelines. The Brigade or unit security manager will notify the COMSEC Manager of the access termination. The unit security manager will identify 5% of the unit for submission into the DACAP program each year and submit to the SSM.

(c) All Security Managers will ensure that DACAP termination requirements are added to the out-processing checklist procedures and modified accordingly.

(d) When derogatory information of an employee results in termination from cryptographic access, unit Security Managers will notify the SSM that the termination is a result of derogatory information and submit an incident report to the central clearance facility (CCF). The COMSEC Manager must be notified when an individual's clearance has been downgraded or revoked.

(e) Deployment or mobilization: A deploying or mobilizing Brigade must manage the DACAP enrollment for all personnel, military or civilian assigned to the Brigade for the length of the deployment or mobilization. The Brigade S-2 will process personnel in the enrollment and termination of DACAP IAW AR 380-40. DACAP information for personnel who are members of the ARNG Brigade's home state will be retained and provided to the state SSM or G2 upon return to their state. Personnel who are not members of the ARNG Brigade's home state will be out briefed and provided their DACAP information for transfer to their home organization in CONUS.

(f) At the end of deployment or mobilization the Brigade S-2 will out process and debrief all attached military or civilian personnel who are not assigned to the Brigade as permanent personnel.

b. Appointing subordinate Security Managers. SSMs or G-2 may appoint, in writing, additional representatives to assist in managing the state's DACAP program as Security Managers. However, ultimate responsibility for the program resides with the SSMs and G-2.

c. Security clearance verification. Security Managers are the only designated personnel authorized to perform security clearance verification.

(1) At a minimum, COMSEC personnel must meet all requirements provided under AR 380-40, para 2-2.

(2) Assigned COMSEC personnel operating Electronic Key Management System (EKMS) or Key Management Infrastructure (KMI) or serving as system administrators and/or platform administrators will require IT Level I access. To be eligible for access, personnel require a favorably adjudicated Single Scope Background Investigation (SSBI) or phased periodic re-investigation.

(3) Coordination with ARNG-HRP, Personnel Division, is required to incorporate best practices for periodic recertification of COMSEC personnel whose position sensitivity would otherwise not support the requisite level of access under this policy.

d. Counterintelligence Scope Polygraph (CSP). The COMSEC account personnel enrolled in DACAP are subject to CSP examination. All personnel submitted into DACAP must have at least 1 year remaining of service eligibility after CSP submission.

(1) The State Security Manager will consolidate the DACAP enrollments using the enclosed spreadsheet IAW AR 380-40, para 7-4. The individual's Social Security Number (SSN) will be used IAW AR 480-40. The spreadsheet will be forwarded to the ARNG G-2 COMSEC Program Manager no later than 1 June of each year. Use of an individual's SSN makes the spreadsheet PII sensitive and requires special protection. Transmission of PII information requires documentation encryption.

(2) CSP testing will require TDY to one of the CSP testing locations. Individual TDY expenses are funded by each state. CSP testing is given at the following locations:

(a) Ft Meade, MD. Call (301) 677-4210 to schedule

(b) Ft Gordon, GA. Call (706) 791-5613 to schedule

(3) ARNG G-2 will centrally manage who is submitted for CSPs to meet the 5% requirement in AR 380-40. The ARNG G-2 COMSEC Program Manager will submit the consolidated ARNG DACAP/CSP spreadsheet no later than 1 September of each year to the Army Intelligence Polygraph and Credibility Assessment (PCA) Program.

(4) CSPs are valid for 5 years. The SSM, G-2, eligible S-2 or unit security will verify each individual has at least 1 year of eligible service remaining after CSPs are submitted. A CSP is not requested for personnel who have a current CSP or if personnel have 1 year or less of remaining service eligibility.

(5) Personnel will be removed from the DACAP enrollment process if they are pending a due process for a security incident.

ARNG-OIZ
SUBJECT: Army National Guard (ARNG) Department of the Army Cryptographic Access Program (DACAP) Policy

6. This policy supersedes Army National Guard (ARNG) Department of the Army Cryptographic Access Program (DACAP) Policy, dated 11 April 2016.

7. My point of contacts are Mr. George S. Bryant Jr., COMSEC Officer, at DSN 329-8127 or (703) 601-8127, george.s.bryant2@mail.mil and Mr. Kevrain K. Ford, Security Programs Branch Chief, at DSN 329-8263 or (703) 607-8263 or kevrain.k.ford.civ@mail.mil and

BRENT L. RICHARDS
COL, GS
G2, Army National Guard

Encl
1: DACAP Enrollment Spreadsheet
2: SD Form 572
3: Cryptographic Access Briefing