

NATIONAL GUARD BUREAU

111 SOUTH GEORGE MASON DRIVE ARLINGTON, VA 22204-1382

ARNG-OIS-C 28 October 2013

MEMORANDUM FOR State, Territories and the District of Columbia ARNG G-2s, G6s and Security Managers

SUBJECT: Army National Guard Policy for the Department of the Army Cryptographic

Access Program (DACAP)

1. References:

a. DODI 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

c. AR 380-67, Personnel Security Program, 9 September 1998

d. AR 25-400-2, The Army Records Management System (ARIMS), 2 October 2007 e. AR 25-2, Information Assurance, 24 October 2007

2. Applicability: This memorandum applies to all Army military and civilian personnel officially assigned to duties that require continuing access to classified cryptographic and COMSEC information.

3. Purpose: To provide the policy and procedures to successfully manage the Department of the Army Cryptographic Access Program (DACAP) using existing lines of authority within the security management hierarchy.

4. Policy: State Security Managers will manage the Department of the Army Cryptographic Access Program (DACAP) in accordance with AR 380-40, chapter 7, and will ensure the unit DACAP points of contact successfully administer the program.

5. Procedures: The DACAP will require State Security Managers to develop procedures that support security clearance verification, cryptographic access/termination certification, and requests for Counterintelligence Scope Polygraphs (CSPs). These procedures include:

ARNG-OIS-C

SUBJECT: Army National Guard Policy for Department of the Army Cryptographic

Access Program (DACAP)

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

(1) Communication Security (COMSEC) personnel must meet all requirements provided under AR 380-40, paragraph 2-2. At a minimum, this requires the security clearance of COMSEC personnel to be equal to the classification associated with the Highest Classification Indicator (HCI) for the COMSEC account.

(2) The COMSEC personnel operating key management infrastructure (KMI) or serving as system administrators and/or platform administrators require IT Level I access. To be eligible for access, these personnel require a favorable adjudication of a Single Scope Background Investigation (SSBI).

(3) Coordination with ARNG-HRP, Personnel Division, may be 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.

b. Cryptographic access/termination certification. All certification and termination briefings for cryptographic access must be completed in accordance with AR 380-40, paragraph 7-4.

(1) Granting cryptographic access:

(a) The cryptographic access certification briefing and the authorization portion of Secretary of Defense (SD) Form 572, Cryptographic Access Certification and Termination, will be completed by the Security Manager. A sample access certification briefing is provided in AR 380-40, Appendix D, and is included in the memorandum format as enclosed. The Security Manager, in accordance with 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.

(b) A copy of the completed SD Form 572 and a copy of the access certification briefing will be provided by the Security Manager to the State Security Manager for documenting DACAP enrollments. In the future, DACAP enrollments may be managed within the Joint Verification System (JVS) Cryptographic Access Program (CAP). Until such time, manual enrollment is required.

ARNG-OIS-C

SUBJECT: Army National Guard Policy for Department of the Army Cryptographic

Access Program (DACAP)

(c) A copy of the completed SD Form 572 and a copy of the access briefing will be provided by the Security Manager to the COMSEC Account Manager for audit and inspection purposes.

(2) Terminating cryptographic access.

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

(b) The Security Manager will provide a copy of the completed SD Form 572 and a copy of the termination certification briefing to his or her State Security Manager for tracking DACAP enrollments. Until the termination briefing and SD Form 572 are complete, personnel will remain enrolled and be subject to CSPs.

(c) The Security Manager will ensure that DACAP termination requirements are added to the out-processing checklist procedures and modified when new guidance is received.

(d) When derogatory information about an employee results in termination of cryptographic access, the Security Manager will notify the State Security Manager that the termination is a result of derogatory information and submit an incident report to the central clearance facility.

c. Counterintelligence Scope Polygraph. The COMSEC account personnel enrolled in DACAP are subject to CSP examination.

(1) The State Security Manager will consolidate the DACAP enrollments for random CSPs in accordance with AR 380-40, paragraph 7-4. Requests for CSPs will be submitted no later than 15 August of each year by the State Security Manager in memorandum format through the NGB G-2, for the Army Intelligence Polygraph and Credibility Assessment (PCA) Program Manager. This memorandum should be limited to 5 percent of the individuals who are enrolled in DACAP as of 1 August of the same year. Only one CSP request from each State or Territory will be accepted annually. The NGB G-2 will forward CSP requests to the Army Intelligence PCA program manager no later than 1 September of the same year.

ARNG-OIS-C

SUBJECT: Army National Guard Policy for Department of the Army Cryptographic

Access Program (DACAP)

(2) The CSPs will not be requested for personnel who have an existing CPS that is current. (The CSP is good for 5 years.) Prior to requesting a CSP, the State Security

Manager must verify that the individual(s) listed on the request does not already have a current CSP.

(3) Personnel must be removed from DACAP enrollment while they are pending due process for a security incident. Because they are not enrolled, they will not be subject to CSPs.

6. The point of contact is CPT Matthew Allen, COMSEC Program Manager, at DSN

329-2205, 703-607-2205, or ng.ncr.arng.list.g2-admin@mail.mil.

*c'JI-.-*

Encl PAUL C. THORN COL, GS

Chief of Staff, Army National Guard

CF:

ARNG G-1

ARNG G-2

ARNG G-6



Department of the Army AND AIR FORCE

JOINT FORCES HEADQUARTERS – NEW YORK

330 Old niskayuna rd

LATHAM, NY 12110-3514

J2 16 February 2017

MEMORANDUM FOR RECORD

SUBJECT: Access/Termination Briefing for Department of the Army Cryptographic

Access Program (DACAP)

1. You have been selected to perform duties that will require access to classified cryptographic information. It is essential that you be made aware of certain facts relevant to the protection of this information before access is granted. You must know the reason why special safeguards are required to protect classified cryptographic information. You must understand the directives that require these safeguards and the penalties you will incur for the unauthorized disclosure and/or retention or negligent handling of classified cryptographic information under the criminal laws of the United States. Failure to properly safeguard this information could cause exceptionally grave damage or irreparable injury to the national security of the United States or could be used to advantage by a foreign nation.

2. Classified cryptographic information is especially sensitive because it is used to protect other classified information. Any particular piece of cryptographic key and any specific cryptographic technique may be used to protect a large quantity of classified information during transmission. If the integrity of a cryptographic system is breached at any point, all information protected by the system may be compromised. The

safeguards placed on classified cryptographic information are a necessary component of Government programs to ensure that our Nation’s vital secrets are not compromised.

3. Because access to classified cryptographic information is granted on a strict need-to- know basis, you will be given access to only that cryptographic information necessary in the performance of your duties. You are required to become familiar with AR 380–40 as well as those publications referenced therein.

4. Especially important to the protection of classified cryptographic information is the timely reporting of any known or suspected compromise of this information to **(J2-Security Office)**. If a cryptographic system is compromised, but the compromise is not reported, the continued use of the system can result in the loss of all information protected by it. If the compromise is reported, steps

can be taken to lessen an adversary’s advantage gained through the compromise of the information.

J2

 SUBJECT: Access/Termination Briefing into Department of the Army Cryptographic

 Access Program (DACAP)

5. As a condition of access to classified cryptographic information, you must acknowledge that you may be subject to a counterintelligence scope polygraph examination. This examination will be administered in accordance with DODD 5210.48 and applicable law. The relevant questions in this polygraph examination concern espionage, sabotage, unauthorized disclosure of classified information, and unreported foreign contacts. If at this time you do not wish to sign such an acknowledgment as a part of executing a cryptographic access certification, this briefing will be terminated and the briefing administrator will so annotate the cryptographic access certificate. Such refusal will not be cause for adverse action, but will result in your being denied access to classified cryptographic information.

6. Intelligence services of some foreign governments prize the acquisition of classified cryptographic information. They will go to extreme lengths to compromise U.S. citizens and force them to divulge cryptographic techniques and materials that protect the Nation’s secrets around the world. Any personal or financial relationship with a foreign government’s representative could make you vulnerable to attempts at coercion to divulge classified cryptographic information. Learn to recognize those attempts so that you may successfully counter them. The best personal policy is to avoid discussions that reveal your knowledge of, or access to, classified cryptographic information and thus avoid highlighting yourself to those who would seek the information you possess. Any attempt, either through friendship or coercion, to solicit your knowledge regarding classified cryptographic information must be reported immediately to (insert appropriate security office).

7. In view of the risks noted above, unofficial foreign travel to foreign countries may require the prior approval of **(J2-Security Office).** It is essential that you contact (**J2-Security Office)** before such unofficial travel.

8. Finally, should you willfully or negligently disclose to any unauthorized persons any of the classified cryptographic information to which you will have access, you may be subject to administrative and civil sanctions, including adverse personnel actions, as

well as criminal sanctions under the UCMJ and or Federal law, as appropriate.

 RUTH J. DERENZO

 SFC, NYARNG

 State Security Manager

 J2

 SUBJECT: Access/Termination Briefing into Department of the Army Cryptographic

 Access Program (DACAP)

Access/Termination Certification Briefing Acknowledgement:

I have received the access and/or termination certification briefing as required by AR

380-40 paragraph 7-4 for DACAP enrollment.

Access Certification: Termination Certification:

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name Printed Name

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Signature

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date Date