CNSS Policy No. 3
October 2007

NATIONAL POLICY

ON

GRANTING ACCESS TO U.S. CLASSIFIED CRYPTOGRAPHIC INFORMATION

Committee on National Security Systems

Chair

FOREWORD

1. Controlling access to the technically sophisticated cryptographic systems employed by the United States Government is a government-wide challenge. The systems can be compromised if individuals are not subject to reasonable controls regarding access to the U.S. classified cryptographic information supporting these systems. This policy supersedes NSTISS Policy No. 3, "National Policy on Granting Access to U.S. Classified Cryptographic Information," dated 19 December 1988.

2. This policy establishes uniform criteria for minimizing the loss or unauthorized disclosure of U.S. classified cryptographic information. The policy makes reference to the possible use of a non-lifestyle, counterintelligence scope polygraph examination. It should be noted, however, that the polygraph is not intended to be used as a prescreening mechanism for determining cryptographic access.

3. In accordance with the Federal Information Security Management Act (FISMA) of 2002, the Committee on National Security Systems (CNSS) Secretariat has initiated an Issuance Compliance Process for reporting annual status of Department and Agency implementation of new/revised CNSS Issuances. The first report for the attached policy is due six months following its issuance.

4. Additional copies of this policy may be obtained from the Secretariat or the CNSS Website – www.cnss.gov.

/s/
John G. Grimes

CNSS Secretariat (I923) . National Security Agency . 9800 Savage Road STE 6716 . Ft Meade MD 20755-6716
(410) 854-6805 . UFAX: (410) 854-6814
cnss@radium.ncsc.mil

NATIONAL POLICY ON GRANTING ACCESS TO U.S. CLASSIFIED CRYPTOGRAPHIC INFORMATION

SECTION I – SCOPE

1. This policy establishes criteria for granting access to SECRET and TOP SECRET cryptographic information that is owned, produced by or for, or is under the control of the U.S. government. The criteria do not apply to CONFIDENTIAL or unclassified cryptographic information.

2. Nothing in this policy shall alter or supersede existing authorities of the Director of National Intelligence (DNI).

SECTION II – REFERENCES

3. References are listed in ANNEX A.

SECTION III – DEFINITIONS

4. Definitions in reference a. apply to this policy; additional terms are defined in ANNEX B.

SECTION IV – POLICY

5. SECRET and TOP SECRET cryptographic information, the loss of which could cause serious or exceptionally grave damage to U.S. national security, requires special access controls. All government departments, agencies and their contractors (consistent with Reference b.) shall establish a formal cryptographic access program where access to SECRET and TOP SECRET cryptographic information shall only be granted to an individual who is assigned to a position that requires access to SECRET or TOP SECRET cryptographic information and satisfies the criteria set forth below:

a. Is a U.S. citizen;

b. Is an employee of the U.S. Government, is a U.S. Government-cleared contractor or employee of such contractor, or is employed as a U.S. Government representative (including consultants of the U.S. Government);

c. Possesses a security clearance appropriate to the classification of the U.S. cryptographic information to be accessed;

d. Receives a security briefing appropriate to the classification of the cryptographic information to be accessed; and,

e. Acknowledges the responsibilities and obligations of access by signing a cryptographic access certificate.

6. Where department or agency heads direct, individuals granted access to cryptographic information under this policy, will be required to acknowledge the possibility of being subjected to a non-lifestyle, counterintelligence scope polygraph examination administered in accordance with department or agency directives and applicable law.

7. All persons indoctrinated for cryptographic access under the policy may be subject to special requirements regarding unofficial foreign travel or contacts with foreign nationals, as prescribed by their respective department or agency security directives.

8. This policy shall apply to all individuals whose official duties require continuing access to U.S. classified cryptographic information. This includes those individuals assigned:

a. As COMSEC custodians or alternates.

b. As producers or developers of cryptographic key or logic.

c. As cryptographic maintenance or installation technicians.

d. To spaces where cryptographic keying materials are generated or stored.

e. To prepare, authenticate, or decode valid or exercise nuclear control orders.

f. In secure telecommunications facilities located in fixed ground facilities or on-board ships.

g. Any other responsibility with access to U.S classified cryptographic information, which is specifically identified by the head of a department or agency.

SECTION V – RESPONSIBILITIES

9. Heads of Federal Departments and Agencies shall:

a. Ensure compliance with the requirements of this policy.

b. Ensure resources are available to implement this policy.

c. Develop and administer a "Cryptographic Access Briefing" addressing the specific security concerns of the department or agency; an example of such a briefing is presented in ANNEX C.

d. Prepare a cryptographic access certification, which shall include a certificate signed by all individuals granted cryptographic access in accordance with this program, such as DoD Form SD-572 or DEA Form 56; an example of such a certificate is presented in ANNEX D. The Cryptographic Access Certificate, with the completed Termination of Access Statement, shall be made a permanent part of the individual's official security records and shall be accounted for in accordance with department or agency directives concerning retention of security clearance/access certificates.

e. Ensure that applicable department or agency security directives contain requirements for reporting unofficial foreign travel and contacts with foreign nationals.

f. Incorporate the content of this policy into personnel training and awareness programs.

Encls:

ANNEX A - References
ANNEX B - Definitions
ANNEX C - Cryptographic Access Briefing (SAMPLE)
ANNEX D - Cryptographic Access Certification (SAMPLE)

ANNEX A

REFERENCES

a. Committee on National Security Systems (CNSS) Instruction No. 4009, "National Information Assurance (IA) Glossary," June 2006 or its successor.

b. Executive Order 12829, "National Industrial Security Program," 16 Sep 1993, as amended.

c. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4001, "Controlled Cryptographic Items," dated July 1996.

ANNEX B

DEFINITIONS OF SPECIALIZED TERMS

Terms used in this policy are defined in Reference a. with the exception of the following:

U.S. CLASSIFIED CRYPTOGRAPHIC INFORMATION:

a. Cryptographic key and authenticators that are classified and are designated as TOP SECRET CRYPTO or SECRET CRYPTO.

b. All cryptographic media that embody, describe, or implement classified cryptographic logic, to include, but not limited to, full maintenance manuals, cryptographic descriptions, drawings of cryptographic logic, specifications describing a cryptographic logic, and cryptographic software, firmware, or repositories of such software such as magnetic media or optical disks.

ANNEX C

SAMPLE
CRYPTOGRAPHIC ACCESS BRIEFING

You have been selected to perform duties that will require access to U.S. 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 U.S. classified cryptographic information. You must understand this directive, which requires these safeguards and the penalties you may incur for the unauthorized disclosure, unauthorized retention, or negligent handling of U.S. classified cryptographic information under the criminal laws of the United States. Failure to properly safeguard this information could cause serious or exceptionally grave damage, or irreparable injury, to the national security of the United States; or could be used to advantage by a foreign nation.

U.S. classified cryptographic information is especially sensitive because it is used to protect other classified information. Any particular piece of cryptographic keying material 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 U.S. classified cryptographic information are a necessary component of government programs to ensure that our nation's vital secrets are not compromised.

Because access to U.S. 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 (insert, as appropriate, department or agency implementing directives governing the protection of cryptographic information). Cited directives are attached in a briefing book for your review at this time.

Especially important to the protection of U.S. classified cryptographic information is the timely reporting of any known or suspected compromise of this information. 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.

NOTE: The following two paragraphs shall only be included when the applicable department or agency head directs.

As a condition of access to U.S. classified cryptographic information, you must acknowledge the possibility that you may be subject to a non-lifestyle, counterintelligence scope polygraph examination. This examination will be administered in accordance with the provisions of (insert appropriate department or agency directive) and applicable law. This polygraph examination will only encompass questions concerning espionage, sabotage, or

questions relating to unauthorized disclosure of classified information.

You have the right to refuse to acknowledge the possibility of being subject to a non-lifestyle, counterintelligence scope polygraph examination. Such refusal will not be cause for adverse action but may result in your being denied access to U.S. classified cryptographic information. If you do not, at this time, wish to sign such an acknowledgement as a part of executing a cryptographic access certification, this briefing will be terminated at this point and the briefing administrator will so annotate the cryptographic access certificate.

You should know that intelligence services of some foreign governments prize the acquisition of U.S. 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. You must understand that any personal or financial relationship with a foreign government's representative could make you vulnerable to attempts at coercion to divulge U.S. classified cryptographic information. You should be alert 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, U.S. 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 U.S. classified cryptographic information must be reported immediately to (insert appropriate security office).

In view of the risks noted above, unofficial travel to designated countries may require the prior approval of (insert appropriate security office). It is essential that you contact (insert appropriate security office) if such unofficial travel becomes necessary.

Finally, you must know that, should you willfully or negligently disclose to any unauthorized persons any of the U.S. 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 Uniform Code of Military Justice (UCMJ) and/or the criminal laws of the United States, as appropriate.

ANNEX D

SAMPLE

CRYPTOGRAPHIC ACCESS CERTIFICATION

INSTRUCTION

Section I of this certification must be executed before an individual may be granted access to U.S. classified cryptographic information. Section II will be executed when the individual no longer requires such access. The signed certificate (original) will be made a permanent part of the official security records of the individual concerned.

SECTION I

AUTHORIZATION FOR ACCESS TO U. S. CLASSIFIED CRYPTOGRAPHIC

INFORMATION

a. I understand that I am being granted access to U.S. classified cryptographic information. I understand that my being granted access to this information involves me in a position of special trust and confidence concerning matters of national security. I hereby acknowledge that I have been briefed concerning my obligations with respect to such access.

b. I understand that safeguarding U.S. classified cryptographic information is of the utmost importance and that the loss or compromise of such information could cause serious or exceptionally grave damage to the national security of the United States. I understand that I am obligated to protect U.S. classified cryptographic information and I have been instructed in the special nature of this information and the reasons for the protection of such information. I agree to comply with any special instructions, issued by my department or agency, regarding unofficial foreign travel or contacts with foreign nationals.

NOTE: The following statement shall only be included when the applicable agency or department head directs.

I acknowledge that I may be subject to a non-lifestyle, counterintelligence scope polygraph examination to be administered in accordance with (insert appropriate department or agency directive) and applicable law.

c. I understand fully the information presented during the briefing I have received. I have read this certificate and my questions, if any, have been satisfactorily answered. I acknowledge that the briefing officer has made available to me the provisions of Title 18, United States Code, Sections 641, 793,794, 798, and 952. I understand that, if I willfully disclose to any unauthorized person any of the U.S. classified cryptographic information to which I might have access, I may be subject to prosecution under the UCMJ and/or the criminal laws of the United States, as appropriate. I understand and accept that unless I am released in writing by an authorized representative of (insert appropriate security office) the terms of this certificate and my obligation to protect all U.S. classified cryptographic information to which I may have access, apply during the time of my access and at all times thereafter.

_____

ACCESS GRANTED THIS DAY OF 20

_____

SIGNATURE NAME/GRADE, RANK, RATING/SSN

_____

SIGNATURE OF ADMINISTERING OFFICIAL NAME/GRADE/OFFICIAL POSITION

SECTION II

TERMINATION OF ACCESS TO U.S. CLASSIFIED

CRYPTOGRAPHIC INFORMATION

I am aware that my authorization for access to U.S. classified cryptographic information is being withdrawn. I fully appreciate and understand that the preservation of the security of this information is of vital importance to the welfare and defense of the United States. I certify that I will never divulge any U.S. classified cryptographic information I acquired, nor discuss with any person, any of the U.S. classified cryptographic information to which I have had access, unless and until freed from this obligation by unmistakable notice from proper authority. I have read this agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available to me Title 18, United States Code, Sections 641, 793, 794, 798, and 952; and Title 50, United States Code, Section 783(b).

_____

ACCESS WITHDRAWN THIS DAY OF

_____

SIGNATURE NAME/GRADE, RANK, RATING

_____

SIGNATURE OF ADMINISTERING OFFICIAL NAME/GRADE/OFFICIAL POSITION