



# governmentattic.org

*"Rummaging in the government's attic"*

Description of document: National Security Agency (NSA) Classification Guide for SHAMROCK; internal histories of SHAMROCK

Requested date: 08-December-2024

Release date: 23-December-2024

Posted date: 27-January-2025

Source of document: FOIA Request  
National Security Agency  
Attn: FOIA/PA Office  
9800 Savage Road, Suite 6932  
Fort George G. Meade, MD 20755-6932  
Fax: 443-479-3612  
[Online Form](#)

The governmentattic.org web site ("the site") is a First Amendment free speech web site and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



NATIONAL SECURITY AGENCY  
FORT GEORGE G. MEADE, MARYLAND 20755-6000

FOIA Case: 119777  
23 December 2024

This responds to your Freedom of Information Act (FOIA) request dated 8 December 2024, for the follow:

- 1) A copy of the classification guide for SHAMROCK, the 1947-1973 program in which certain international telegraph/cable traffic transmitted on Western Union, RCA Global, and/or ITT World Communications' international facilities was made available to the U.S. Government, which was a continuation of the military censorship program of World War II.
- 2) NSA Classification Guide 389-00 3) a copy of each internal history of the SHAMROCK program. If any of these documents are classified, review them for declassification in part or whole.

Your request was received on 9 December 2024, and assigned Case Number 119777. There are no assessable fees for this request; therefore, we did not address your fee category. NSA has processed your request under the provisions of the FOIA.

We have completed our search for records responsive to your request and the documents you requested are enclosed. Certain information, however, has been protected in the enclosure.

Some of the information was protected from the document was found to be currently and properly classified in accordance with Executive Order 13526. This information meets the criteria for classification as set forth in Subparagraph (c) of Section 1.4 and remains classified as provided in Section 1.2 of the Executive Order. The information is classified because its disclosure could reasonably be expected to cause exceptionally grave damage to the national security. The information is exempt from automatic declassification in accordance with Section 3.3(b)(1) of E.O. 13526. Because the information is

currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)).

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in these documents. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Section 6, Public Law 86-36 (50 U.S. Code 3605).

Finally, personal information regarding an individual has been withheld from the enclosures in accordance with 5 U.S.C. 552 (b)(6). This exemption protects from disclosure information that would constitute a clearly unwarranted invasion of personal privacy. In balancing the public interest for the information you request against the privacy interests involved, we have determined that the privacy interests sufficiently satisfy the requirements for the application of the (b)(6) exemption.

You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below. NSA will endeavor to respond within 20 working days of receiving any appeal, absent any unusual circumstances.

- The appeal must be sent via U.S. postal mail, fax, or electronic delivery (e-mail) and addressed to:

NSA/CSS FOIA/PA Appeal Authority (P132)  
National Security Agency  
9800 Savage Road STE 6932  
Fort George G. Meade, MD 20755-6932

The facsimile number is (443)479-3612.

The appropriate email address to submit an appeal is  
FOIA\_PA\_Appeals@nsa.gov.

- It must be postmarked or delivered electronically no later than 90 calendar days from the date of this letter. Decisions appealed after 90 days will not be addressed.
- Please include the case number provided above.
- Please describe with sufficient detail why you believe the denial of requested information was unwarranted.

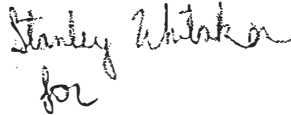
You may also contact our FOIA Public Liaison at foialo@nsa.gov for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the

National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services  
National Archives and Records Administration  
8601 Adelphi Rd. - OGIS  
College Park, MD 20740  
ogis@nara.gov  
877/684-6448  
202/741-5769

Correspondence related to your request should include the case number assigned to your request, which is included in the first paragraph of this letter. Your letter should be addressed to National Security Agency, FOIA Division (P132), 9800 Savage Road STE 6932, Ft. George G. Meade, MD 20755-6932 or may be sent by facsimile to 443-479-3612. If sent by fax, it should be marked for the attention of the FOIA Division. The telephone number of the FOIA Division is 301-688-6527.

Sincerely,



Stanley Whitaker  
for

SALLY A. NICHOLSON  
Chief, FOIA/PA Division  
NSA Initial Denial Authority

Encls:  
a/s

by [redacted] to

Capt. Morris from Capt W

Please give me coverage

delays in receipt of traffic

from the various Chambers

and

Approved for Release by NSA on 03-27-2014,  
EOIA Case # 70768

#### 4. Operation SHAMROCK

SHAMROCK is the name of a source of foreign intelligence information from which the National Security Agency (NSA) received from RCA Global, ITT World Communications, and Western Union International copies of certain international telegrams handled on their facilities. Copies of these telegrams were initially received in the form of microfilm or paper tapes and, subsequently, in the case of RCA Global and ITT World Communications, in the form of magnetic tapes. Where copies of microfilm were used to provide materials to NSA, if any, only certain foreign communications were so provided. Where magnetic tape was used to provide materials to NSA, the focus by NSA continued to be on foreign communications and foreign governments. The carriers were engaged in transmitting or receiving foreign communications only.

Telegraphic messages that were obtained from the aforementioned carriers, were, in turn, screened by classified and carefully protected procedures pursuant to the Agency's foreign intelligence requirements imposed upon the Agency by the United States Intelligence Board. Pursuant to these requirements, and as described above in Subsection 3, from 1967 to 1973, Federal agencies provided NSA with names of individuals and organizations commonly referred to as "watch lists."

The SHAMROCK source was not the only means used by the NSA to obtain international communications to fulfill its foreign intelligence mission.

After a telegraphic message was selected pursuant to the foregoing foreign intelligence requirements placed on NSA, the information contained in the message was extracted and in general edited or summarized to conceal its source in order to produce an intelligence report. All watch list reports were edited or summarized to conceal their source. These methods of processing and selection were identical for all sources of information used to produce foreign intelligence and were not limited to the SHAMROCK source.

NSA did not retain the "raw" copy of original texts of telegraphic material received, in whatever form, from the

international common-access carriers; it retained and distributed only the edited or summarized product. Because the source of the telegraphic material was not included in the watch list reports, it was and is not possible to ascertain whether such material had been derived from the SHAMROCK source. (Nor can that material be identified as having been received from a particular common-access carrier.)

The common-access carriers were not informed as to what was done with the information in the material they provided. Common-access carrier officials have testified in other forums that they do not retain for any significant period "raw" copies or reproductions in any form of the original text of communications transmitted by them.



Approved for Release by NSA, FOIA Case # 18871

UNCLASSIFIED // FOR OFFICIAL USE ONLY

**(U) SHAMROCK and MINARET Classification Guide, 389-00**

**CLASSIFICATION GUIDE NUMBER: (U) 389-00, SHAMROCK and MINARET  
(NSA Intelligence Activities Revealed in Church/Pike Committee Hearings)**

**PUBLICATION DATE: (U) 30 August 2000**

**OFFICE OF ORIGIN: (U) N5P52**

**POC: (U//FOUO) [redacted] SP52**

**PHONE: (U) 963-4582s**

**ORIGINAL CLASSIFICATION AUTHORITY: (U) JoAnn Grube, Chief, Office of Policy**

Description of Information	Classification/Markings	Reason	Declass	Remarks
(U) The information in this classification guide pertains to specific facts derived from public testimony. Any details of SHAMROCK or MINARET activity not addressed in this guide should be referred to NSP52, Information Security Policy, for determination.				
<b>(U) A. HISTORICAL ACTIVITY</b>				
(U) A.1. The fact that the U.S. has intercepted, analyzed, and in some cases decoded foreign communications since the Revolutionary War.	UNCLASSIFIED			
(U) A.2. The fact that during the Civil War and WWI, the U.S. intercepted foreign telegrams sent by wire.	UNCLASSIFIED			
(U) A.3. The fact that elements of the military have been assigned the task of obtaining intelligence from foreign radio transmissions since the 1930s.	UNCLASSIFIED			
(U) A.4. The fact that during WWII, the U.S. Army and Navy intercepted and analyzed enciphered/coded radio messages.	UNCLASSIFIED			
(U) A.5. The fact that during WWII, all international telegraph traffic was screened by military censors, located at telegraph companies, as part of a censorship program. Messages from foreign intelligence targets were turned over to military intelligence.	UNCLASSIFIED			
<b>(U) B. NSA- GENERAL</b>				
(U) B.1. The fact that signals are intercepted by many techniques and processed, sorted, and analyzed by procedures that reject inappropriate or unnecessary	UNCLASSIFIED			

signals.				
(U) B.2. The fact that lists of words, including names, subjects, locations, etc. are used to sort out information of foreign intelligence value from that which is not of interest.	UNCLASSIFIED			
(U) B.3. The fact that unwanted messages (for example, between two U.S. citizens) are rejected as early in the selection process as possible.	UNCLASSIFIED			
(U) B.4. The fact that NSA confines its activities to communications involving at least one foreign terminal, and excludes communications between U.S. citizens or entities.	UNCLASSIFIED			
(U) B.5. The fact that directives now in effect in various agencies preclude resumption of collection activity based on the names of U.S. citizens unless personally approved by the Attorney General.	UNCLASSIFIED			
<b>(U) C. SHAMROCK - PARTICIPATING AGENCIES AND COMPANIES</b>				
(U) C.1. The fact that the term SHAMROCK was given to a message collection program in which the Government persuaded three international telegraph companies - RCA Global, ITT World Communications, and Western Union International, to make available in various ways certain of their international telegraph traffic to the U.S. Government.	UNCLASSIFIED			
(U) C.2. The fact that SHAMROCK was a continuation of the military censorship program of WWII.	UNCLASSIFIED			
(U) C.3. The fact that the Army Security Agency (ASA) was the first Government agency responsible for SHAMROCK. When the Armed Forces Security Agency (AFSA) was created in 1949, it inherited the program, as did NSA on its creation in 1952.	UNCLASSIFIED			
(U) C.4. The fact that SHAMROCK operated from 1947-1973, and involved use of Watch Lists 1967-1973.	UNCLASSIFIED			(U) See MINARET section for guidance on Watch List activity.
(U) C.5. The fact that initially, the Government only used the telegrams relating to certain foreign targets, and then began to extract telegrams of certain U.S. citizens.	UNCLASSIFIED			
(U) C.6. The fact that while the original purpose of SHAMROCK was to obtain	UNCLASSIFIED			

foreign intelligence, programs frequently did not distinguish between messages of foreigners and messages of U.S. citizens.				
(U) C.7. The fact that RCA Global, ITT World Communications, and Western Union International were not paid for their services to SHAMROCK.	UNCLASSIFIED			
(U) C.8. The fact that only the Director, Deputy Director, and a lower-level manager at NSA had operational responsibility for SHAMROCK at any one time.	UNCLASSIFIED			
(U) C.9. The fact that each of the companies involved limited knowledge of SHAMROCK to two or three individuals due to concerns regarding the legality of the operation.	UNCLASSIFIED			
(U) C.10. The fact that Secretary of Defense Forrestal gave assurances in December 1947, saying he was speaking on behalf of the President and the Attorney General, that the companies involved would not be subject to criminal prosecution as long as "the current administration" was in office. Secretary of Defense Johnson provided the same assurances in 1949.	UNCLASSIFIED			
(U) C.11. The fact that President Truman, Attorney General Tom Clark, and Secretary of Defense Schlesinger were aware of and approved of Project SHAMROCK.	UNCLASSIFIED			
(U) C.12. The fact that offices of RCA Global, ITT World Communications, and Western Union International in New York City, NY; Washington DC; San Francisco, CA; San Antonio, TX; and Miami, FL participated in SHAMROCK.	UNCLASSIFIED			
(U) C.13. The fact that approximately 90% of the messages collected for SHAMROCK came from New York City, NY.	UNCLASSIFIED			
(U) C.14. The fact that in the beginning, the Government received paper tapes of messages that had been transmitted by overseas cables, as well as microfilm copies of messages that had been sent by radio.	UNCLASSIFIED			
(U) C.15. The fact that NSA never received domestic telegrams from the companies involved.	UNCLASSIFIED			(U) None of the companies had operations which included passing

				telegrams within the United States after 1963.
(U) C.16. The fact that the government did not tell the companies that it was extracting telegrams of certain U.S. citizens.	UNCLASSIFIED			
(U) C.17. The fact that RCA Global and ITT World Communications provided NSA with the bulk of their international message traffic, which NSA then selected for traffic of foreign intelligence targets.	UNCLASSIFIED			
(U) C.18. The fact that in the 1960s, RCA Global and ITT World Communications began to store their international paid message traffic on magnetic tapes, which were turned over to NSA.	UNCLASSIFIED			
(U) C.19. The fact that NSA made copies of magnetic tapes in its rented office space in New York City, NY.	UNCLASSIFIED			
(U) C.20. The fact that Western Union International sorted the traffic itself and provided NSA only with copies of the traffic of certain foreign targets and all the traffic to one country.	UNCLASSIFIED			(U) Information regarding foreign entities targeted shall be classified in accordance with existing guidance.
(U) C.21. The fact that Western Union International microfilmed copies of outgoing international telegrams for pickup by a government courier.	UNCLASSIFIED			
(U) C.22. The fact that in Washington, DC, the companies turned over copies of particular traffic to the FBI, who then passed it to NSA.	UNCLASSIFIED			
<b>(U) D. MINARET - REQUESTING AGENCIES AND SUBJECT MATTER</b>				
<b>NOTE: (U) Names included on Watch Lists are the equity of the submitting agency and may not be released without referral to that agency.</b>				
(U) D.1. The fact that the term MINARET was used beginning in 1969 for Watch List activity which had begun in 1967 and lasted through 1973.	UNCLASSIFIED			
(U) D.2. The fact that MINARET was conducted in response to requirements levied by its customers.	UNCLASSIFIED			
(U) D.3. The fact that from 1967-1969, "the procedure for submitting names was more informal"; starting in 1969, the procedure was formalized and the names for Watch Lists were submitted through channels in writing.	UNCLASSIFIED			

(U) D.4. The fact that there were no warrants obtained for any of the intercepts of U.S. citizens for Watch List activity.	UNCLASSIFIED			
(U) D.5. The fact that the information produced by MINARET was, with one exception, entirely a by-product of NSA's foreign intelligence mission.	UNCLASSIFIED			
(U) D.6. The fact that the one instance in which foreign messages were intercepted specifically for MINARET purposes occurred as follows: The collection was of telephone calls passed over international communications facilities between the United States and South America. The collection was at the request of the Bureau of Narcotics and Dangerous Drugs (BNDD) to produce intelligence information on the methods and locations of foreign narcotics trafficking.	UNCLASSIFIED			
(U) D.7. The fact that NSA asked CIA to assist in the collection as described in the previous entry. This lasted for approximately 6 months, late 1972-early 1973, when CIA stopped due to concern that the activity exceeded CIA statutory restrictions.	UNCLASSIFIED			
(U) D.8. The fact that during the early 1960s, requesting agencies asked NSA to look for reflections in international communications of certain U.S. citizens traveling to Cuba.	UNCLASSIFIED			
(U) D.9. The fact that beginning in 1967, requesting agencies provided names of citizens and organizations (some of which were U.S. citizens and organizations) in an effort to obtain information which was available in foreign communications as a by-product of NSA's normal foreign intelligence mission.	UNCLASSIFIED			
(U) D.10. The fact that from 1967-1973, requirements for Watch Lists were developed in four basic areas: International Drug Trafficking, Presidential Protection, Terrorism, and Possible Foreign Support or Influence on Civil Disturbances.	UNCLASSIFIED			
(U) D.11. The fact that the CIA submitted Watch Lists covering requirements on international travel, foreign influence, foreign support of so-called U.S. extremists and terrorists, and U.S. persons active in the anti-war movement	UNCLASSIFIED			(U) These lists included approximately 30 U.S. citizens and approximately 700 foreign individuals and groups.

<p>(U) D.12. The fact that the FBI submitted Watch Lists to NSA covering requirements on foreign ties and support to certain U.S. citizens and groups. These lists contained names of so-called extremist persons and groups, individuals and groups active in civil disturbances, and terrorists.</p>	UNCLASSIFIED			<p>(U) These lists included approximately 1,000 U.S. citizens and approximately 1,700 foreign individuals and groups.</p>
<p>(U) D.13. The fact that the DIA submitted a Watch List covering requirements on possible foreign control of, or influence on, U.S. anti-war activity. The list contained names of individuals traveling to North Vietnam.</p>	UNCLASSIFIED			<p>(U) This list included approximately 20 U.S. citizens.</p>
<p>(U) D.14. The fact that the Secret Service submitted a Watch List covering requirements in support of their efforts to protect the President and other senior officials.</p>	UNCLASSIFIED			<p>(U) This list contained names of persons thought to be a threat to Secret Service protectees, as well as the names of the protectees themselves.</p> <p>(U) This list included approximately 180 U.S. citizens and approximately 525 foreign individuals and groups.</p>
<p>(U) D.15. The fact that the BNDD submitted a Watch List in 1970 covering requirements related to foreign sources of drugs and foreign organizations and methods used to introduce illicit drugs into the United States.</p>	UNCLASSIFIED			<p>(U) This list contained names of suspected drug traffickers.</p> <p>(U) This list included approximately 450 U.S. citizens and over 3,000 foreign individuals.</p>
<p>(U) D.16. The fact that the Army requested from NSA any available information on foreign influence over, or control of, civil disturbances in the U.S.</p>	UNCLASSIFIED			
<p>(U) D. 17. The fact that, between 1967 and 1973, there was a cumulative total of approximately 450 U.S. persons on the Narcotics List, and about 1,200 U.S. names on all other lists combined.</p>	UNCLASSIFIED			
<p>(U) D. 18. The fact that, at the height of the Watch List activity, there were approximately 800 U.S. citizens on the Watch List, approximately one-third of which were on the Narcotics List.</p>	UNCLASSIFIED			
<p>(U) D.19. The fact that, between 1967 and 1973, approximately 2,000 reports were issued by NSA on international narcotics trafficking, and about 1,900 reports were issued covering</p>	UNCLASSIFIED			

terrorism, executive protection and foreign influence over U.S. groups. This equates to approximately 2 reports per day.				
(U) D.20. The fact that a major terrorist act in the U.S. was prevented due in part to MINARET reporting.	UNCLASSIFIED			(U) Details regarding the terrorist act shall be classified in accordance with existing guidance.
(U) D.21. The fact that some large drug shipments were prevented from entering the U.S. due in part to MINARET reporting.	UNCLASSIFIED			
<b>(U) E. LOCATIONS</b>				
(U) E.1. The fact that CIA provided an office in New York City, NY to NSA 1966-1973 for the purpose of copying telegrams.	UNCLASSIFIED			
(U) E.2. The fact that NSA found accommodation in New York City, NY after the CIA pulled out of the arrangement in 1973.	UNCLASSIFIED			
(U) E.3. The fact that a courier traveled to New York City, NY each day from Ft. Meade, MD to bring back paper/magnetic tapes containing copies of international telegrams sent from New York City, NY the previous day using the facilities of RCA Global, ITT World Communications, and Western Union International.	UNCLASSIFIED			
<b>(U) F. NSA PROCESSING OF SHAMROCK AND MINARET MATERIAL</b>				
(U) F.1. The fact that MINARET activity consisted of scanning international communications already intercepted for other purposes to derive information which met MINARET requirements.	UNCLASSIFIED			
(U) F.2. The fact that all MINARET collection was conducted against international communications with at least one terminal in a foreign country. The foreign terminal (with one exception) was the initial object of collection.	UNCLASSIFIED			(U) Information regarding foreign entities targeted shall be classified in accordance with existing guidance.  (U) See item 38.
(U) F.3. The fact that, of the 2,000 reports issued 1967-1973 on international narcotics trafficking and the 1,900 reports issued during the same time period on terrorism, executive protection, and foreign influence on U.S. groups, over 90% had at least one foreign communicant and all had at least one foreign terminal.	UNCLASSIFIED			

<p>(U) F.4. The fact that NSA personnel made analytic amplifications on Watch List submissions to enhance the selection process.</p>	<p>UNCLASSIFIED</p>			<p>(U) For example, aliases and addresses of persons and organizations on the Watch List were added.</p> <p>(U) Aliases and addresses, as identifiers of the names themselves, are the equity of the submitting agency and may not be released without referral to that agency.</p>
<p>(U) F.5. The fact that paper tapes of messages that had been transmitted by overseas cables and microfilm copies of messages sent by radio were sorted by hand for certain foreign intelligence targets; such traffic could be readily identified by special codes in the heading of each telegram.</p>	<p>UNCLASSIFIED</p>			
<p>(U) F.6. The fact that the magnetic tapes were processed for items of foreign intelligence interest, typically telegrams sent by foreign establishments in the United States or telegrams that appeared to be encrypted.</p>	<p>UNCLASSIFIED</p>			
<p>(U) F.7. The fact that it is estimated that in the later years, NSA selected about 150,000 messages a month for review. Thousands of these messages were disseminated to other agencies.</p>	<p>UNCLASSIFIED</p>			
<p>(U) G. DISSEMINATION OF SHAMROCK AND MINARET INFORMATION</p>				
<p>(U) G.1. The fact that very strict controls were placed on handling of MINARET information.</p>	<p>UNCLASSIFIED</p>			
<p>(U) G.2. The fact that receiving agencies were clearly instructed that MINARET information could not be used for prosecutive or evidentiary purposes.</p>	<p>UNCLASSIFIED</p>			
<p>(U) G.3. The fact that MINARET material was delivered only to designated offices in receiving agencies in order to minimize the risk that the information would be used for purposes other than foreign intelligence.</p>	<p>UNCLASSIFIED</p>			<p>(U) In this instance, the "receiving agencies" are considered to be the same agencies that submitted names for Watch Lists. See "Requesting Agencies and Subject Matter."</p> <p>(U) For example, the BNDD had responsibilities for domestic drug law enforcement as well as for working to curtail international narcotics trafficking. Watch List information supported</p>



				only the latter function.
(U) G.4. The fact that, 1967-1969, information from MINARET activity relating to international messages between U.S. citizens or organizations was issued for background use only and hand-delivered to requesting agencies.	UNCLASSIFIED			
(U) G.5. The fact that, 1967-1969, if the U.S. citizen or organization were only one correspondent of the international communication, the information was published as a normal product report but in a special series to limit distribution.	UNCLASSIFIED			
(U) G.6. The fact that, starting in 1969, information dealing with executive protection and foreign influence over U.S. citizens and groups were provided for background use only and hand-carried to requesting agencies.	UNCLASSIFIED			
(U) G.7. The fact that, when requirements were received in 1970 to supply intelligence regarding international drug trafficking and in 1971 to supply intelligence regarding international terrorism, the information was provided for background use only and hand-carried to requesting agencies.	UNCLASSIFIED			
<b>(U) H. TERMINATION OF SHAMROCK/MINARET</b>				
(U) H.1. The fact that SHAMROCK was terminated by order of the Secretary of Defense, and the Senate Select Committee began studying SHAMROCK in May 1975.	UNCLASSIFIED			
(U) H.2. The fact that concern regarding NSA's role in MINARET activities increased in 1973 due to the following three factors: 1. Concerns that it might not be possible to distinguish definitely between the purpose for the intelligence gathering which was served by the requirements, and the missions and functions of the departments and agencies receiving the information and 2. Concerns that requirements from such agencies were growing and 3. Concern that new, broad discovery procedures in court cases were coming into use which might lead to disclosure of sensitive intelligence sources and methods.	UNCLASSIFIED			
(U) H.3. The fact that MINARET activity which involved U.S. citizens ceased	UNCLASSIFIED			



operationally in the summer of  
1973, and was terminated  
officially in the fall of 1973.

Page Created: October 6, 2000  
Page Last Updated: 10/06/00 11:38:00

**Changes:**



[Back to N5P52 Main Page](#)



~~(U//FOUO)~~ If you have any questions about the content of this page,  
send feedback to [redacted] 963-4582s.

~~(U//FOUO)~~ If you have any questions about this Web page,  
send feedback to [redacted] 963-4582s.

UNCLASSIFIED // FOR OFFICIAL USE ONLY

PUBLICLY RELEASED INFORMATION ON NSA FUNCTIONS AND ACTIVITIES

(NOTE: All of the information contained herein was extracted from public affidavits prepared by NSA and from the testimony of NSA officials before committees of the Senate and the House of Representatives.)

I. Background

NSA was established by Presidential Directive in October 1952 as a separately organized Agency within the Department of Defense under the direction, authority, and control of the Secretary of Defense who was designated by the President as Executive Agent of the Government for conducting the communications security activities and signals intelligence of the United States.

NSA has two primary missions directed to foreign intelligence: (a) a communications security mission and (b) a signals intelligence mission. The communications security mission is to provide the United States Government with the cryptographic equipment, codes, crypto-materials, and procedures to ensure that classified United States communications are protected from the intelligence activities of foreign governments. In fulfilling that mission, the Agency develops codes, coding machines, and coding materials. In addition classified messages

transmitted by any element of the Government are transmitted over systems developed by NSA. The second mission, the signals intelligence mission, is to obtain information from foreign electromagnetic signals and to provide reports derived from such information or data on a rapid response basis to national policymakers and the intelligence community of the United States Government.

## II. FOREIGN INTELLIGENCE MISSION

### 1. General Information

As an intelligence agency, NSA's mission is, quite simply, the production and dissemination of an extremely broad range of signals intelligence (SIGINT) information. This mission is global in scope, and involves information concerning subject matters, foreign officials and entities as varied as the innumerable issues and decisions confronted by policy-making officials of our Government in the area of foreign relations and national defense. The NSA responds essentially to information needs expressed by military and civilian authorities of the Government. Many of NSA's resources are keyed to tasks that support combatant forces. Information needs are derived from two basic sources. First, there are the very broad intelligence objectives and priorities which are identified as a result of

work by bodies like the National Security Council and the President's Foreign Intelligence Advisory Board. These objectives and priorities come to NSA in the form of policies which guide overall resource application. One such objective, for example, is to provide the nation advance warning of military attack, and NSA endeavors to collect information which will contribute to an assessment of that possibility. Second, there are specific information needs which are identified directly to NSA by other governmental or military authorities, and which are satisfied without any reallocation of resources. An example might be to contribute to intelligence support to a military exercise or action.

When a need for information is approved, NSA accepts it as a "requirement." A requirement might best be defined as a statement of an information need from an authorized source which NSA believes it is capable of satisfying within the constraints of its authorities and resources, and which it has, therefore, accepted as a task. The NSA does not generate its own requirements for foreign intelligence.

Upon receipt of such a statement of information need, NSA examines its on-going operation, its authorities and data base, and then performs such processing or reporting as may be necessary to satisfy that need. The Agency's SIGINT activities

include the targeting of foreign governments' communications both within their borders and to and from communicants abroad involving the use of their own radio transmitter and receiver facilities not available for public use. Such communications links are known as "government net" communications. A foreign government may use other means for sending and receiving international radio communications in addition to or instead of its own government facilities. (International radio communications as used here includes communications passed at least in part by wire.) This involves the foreign government's use of the facilities of an international communications common-carrier which are also available for use by the public. Such common-access carriers supply the means by which more than half the encrypted and plain text radio communications of foreign governments, foreign organizations, and their representatives are carried.

It is common knowledge that the total volume of radio signals transmitted on a given day is vast. It is also generally known that radio transmissions can be received by anyone operating the proper receiving equipment in the right place at the right time. Thus, the fact that NSA can intercept radio communications is generally known. So, too, it is known to foreign officials that such interception of radio communications is a primary mission of the NSA. Foreign officials may be

expected to know, also, that NSA cannot possibly intercept even a significant percentage of all such communications, especially taking account of the fact that NSA's activities involve worldwide communications, not solely those having a United States terminal. The number is simply too vast to be handled with any reasonable amount of personnel and equipment. Moreover, the cost and effort of such interception would be disproportionate to the intelligence value of the results.

Instead as NSA's foreign intelligence targets presumably know well -- NSA must focus its interception activities on those particular communications lines, channels, links or systems which yield the highest proportion of useful foreign intelligence information. What foreign government officials do not know, however, is which of the vast number of radio communications NSA attempts to intercept, which are intercepted, and, of those that are intercepted, which yield to NSA processing methods and techniques.

The continued efficacy of NSA's vital intelligence activities requires that the lines, channels, links and systems actually monitored remain unidentified. If a foreign government obtains sufficient reason to suspect that NSA is able to intercept and process that government's radio communications, that government would be expected to take immediate steps to

defeat that capability. This can be accomplished in a number of ways. A foreign government might shift to communications links the U.S. cannot intercept. It may also choose to use alternate methods of communications. The foreign governments may possess the technical capability to either upgrade or initiate cryptography to secure its communications. Finally, a communication channel believed to be targeted by NSA can be used by a foreign government to pass misleading information.

If a foreign power is successful in defeating an interception operation, all of the intelligence from that source is lost unless and until NSA can establish a new and equivalent intercept. The risk involved is great. The information produced by NSA includes political, economic, scientific and military data which is of immeasurable value to the President, the Secretary of Defense, the Secretary of State and other policymakers. Obviously, if a SIGINT source used by the Agency becomes unavailable, policymakers must operate without the information that source produced. Sometimes it is impossible to establish a new and equivalent intercept and the source is lost permanently. Those losses are not only extremely harmful to the national security but also impose a heavy burden on the limited resources of NSA which must attempt to recover the old source or establish an equivalent source of information.



Even after targeting only a small proportion of all available electromagnetic communications for interception, the number of messages intercepted is extremely large. NSA is thus faced with a considerable task in selecting out those messages that will be reviewed for possible intelligence interest. The manner in which NSA does this selection and the degree of reliability and success its methods enjoy are subjects about which virtually no authoritative information has ever been released to the public. Information about these subjects would enable foreign observers to further assess, and thus take steps to defeat, the capabilities of NSA's intelligence gathering techniques.

### 3. Incidental Interception of Private Communications

Because of the nature and capability of the systems involved, NSA's signals intelligence activities to produce foreign intelligence information have unavoidably resulted in the interception of certain other communications sent to or received from a foreign address over international facilities. If a particular communication circuit is known to have been used for the transmission of foreign communications, and monitoring of such communications has been determined to be necessary for national security purposes, the traffic on that circuit will be monitored and recorded. In many instances the same circuits

which NSA monitors for foreign intelligence purposes also are used for the transmission of other communications in which NSA does not have a specific interest. Since NSA cannot, in advance, be aware of the content of specific messages which a sender introduces into the international communications system, there is no way to avoid the interception of some private communications carried over monitored links. These communications are not ordinarily processed, however, since NSA has no interest in communications other than those of a foreign intelligence nature.

### 3. Watch List Activities

The use of lists of words, including individual names, subjects, locations, et cetera, has long been one of the methods used to sort out information of foreign intelligence value from that which is not of interest. In the past, such lists have been referred to occasionally as watch lists, because the lists were used as an aid to watch for foreign activity of reportable intelligence interest. These lists generally did not contain names of U.S. citizens or organizations. Between 1967 and 1973, however, U.S. names were used systematically as a basis for selecting messages, including some between U.S. citizens, when one of the communicants was at a foreign location. In 1969, these activities were dubbed Project MINARET.

Beginning in 1967, certain federal agencies requested that NSA provide to them any information obtained during the course of its foreign signals intelligence activities which indicated foreign influences on specified activities of interest to those agencies, particularly in the areas of Presidential protection and domestic civil disturbances. Later, these activities of interest were extended to include international drug trafficking and acts of terrorism. The requesting agencies included the Secret Service, the Bureau of Narcotics and Dangerous Drugs, the Army, the FBI, the CIA, and the DIA. In aid of their intelligence requirements, the requesting agencies provided NSA with the names of United States and foreign citizens and organizations associated with the aforementioned areas of interest. In response to these requests, NSA would search through its already acquired foreign communications for communications addressed to, originated by, or concerning a particular named individual or organization. If any information was available concerning the requested individual or organization, NSA would forward a summary of that information to the requesting agency.

Between 1967 and 1973 there was a cumulative total of about 450 U.S. names on the narcotics list, and about 1,200 U.S. names on all other lists combined. At the height of the watch list activity, there were almost 800 U.S. names on the watch

list and about one-third of these 800 were from the narcotics list.

Over this six-year period, 1967-1973, about 2,000 reports were issued by NSA on international narcotics trafficking, and about 1,900 reports were issued covering the three areas of terrorism, Executive protection, and foreign influence over U.S. groups. These reports included some messages between U.S. citizens, but over 90 percent had at least one foreign communicant and all messages had at least one foreign terminal. Using agencies did periodically review, and were asked by the NSA to review, their watch lists to insure inappropriate or unnecessary entries were promptly removed.

NSA personnel sometimes made analytic amplifications on customer watch list submissions in order to fulfill certain requirements. For example, when information was received that a name on the watch list used an alias, the alias was inserted; or when an address was uncovered of a watch list name, the address was included. This practice by analysts was done to enhance the selection process, not to expand the lists.

All collection was conducted against international communications with at least one terminal in a foreign country, and, with one exception, for purposes unrelated to the watch list

activity. That is, the communications were obtained, for example, by monitoring communications to and from Hanoi. The one exception in which foreign messages were intercepted for specific watch list purposes was the collection of some telephone calls passed over international communications facilities between the United States and South America. The collection was conducted at the specific request of the Bureau of Narcotics and Dangerous Drugs to produce intelligence information on the methods and locations of foreign narcotics trafficking.

For the period 1967-1969, international messages between United States citizens and organizations selected pursuant to the aforementioned requests were issued to requesting agencies for background use only; however, if a United States citizen or organization were only one party to the international communication, the report derived therefrom was published as a normal intelligence product report but in a special limited distribution series. Beginning in 1969, any international messages that fell into the categories of executive protection and foreign influence over United States citizens and groups were treated in a more restricted fashion than previously, being issued to requesting agencies on a background use only basis. Reports responding to requirements on international drug trafficking and international terrorism, dissemination of which

was begun in 1970 and 1971 respectively, were handled in a similar restricted manner. In the summer of 1973 dissemination of reports to the Bureau of Narcotics and Dangerous Drugs pursuant to that agency's requests was terminated; disseminations of reports pursuant to requests of other agencies in the other previously described areas of interest were terminated by NSA not later than October 1, 1973.

#### 4. Operation SHAMROCK

SHAMROCK is the name of a source of foreign intelligence information from which the National Security Agency (NSA) received from RCA Global, ITT World Communications, and Western Union International copies of certain international telegrams handled on their facilities. Copies of these telegrams were initially received in the form of microfilm or paper tapes and, subsequently, in the case of RCA Global and ITT World Communications, in the form of magnetic tapes. Where copies of microfilm were used to provide materials to NSA, if any, only certain foreign communications were so provided. Where magnetic tape was used to provide materials to NSA, the focus by NSA continued to be on foreign communications and foreign governments. The carriers were engaged in transmitting or receiving foreign communications only.

Telegraphic messages that were obtained from the aforementioned carriers, were, in turn, screened by classified and carefully protected procedures pursuant to the Agency's foreign intelligence requirements imposed upon the Agency by the United States Intelligence Board. Pursuant to these requirements, and as described above in Subsection 3, from 1967 to 1973, Federal agencies provided NSA with names of individuals and organizations commonly referred to as "watch lists."

The SHAMROCK source was not the only means used by the NSA to obtain international communications to fulfill its foreign intelligence mission.

After a telegraphic message was selected pursuant to the foregoing foreign intelligence requirements placed on NSA, the information contained in the message was extracted and in general edited or summarized to conceal its source in order to produce an intelligence report. All watch list reports were edited or summarized to conceal their source. These methods of processing and selection were identical for all sources of information used to produce foreign intelligence and were not limited to the SHAMROCK source.

NSA did not retain the "raw" copy of original texts of telegraphic material received, in whatever form, from the

international common-access carriers; it retained and distributed only the edited or summarized product. Because the source of the telegraphic material was not included in the watch list reports, it was and is not possible to ascertain whether such material had been derived from the SHAMROCK source. (Nor can that material be identified as having been received from a particular common-access carrier.)

The common-access carriers were not informed as to what was done with the information in the material they provided. Common-access carrier officials have testified in other forums that they do not retain for any significant period "raw" copies or reproductions in any form of the original text of communications transmitted by them.

### III. Agency Reliance on Computers

Automatic data processing equipment is indispensable in accomplishing the security and intelligence responsibilities of the National Security Agency. By complicated classified programming instructions computers are used to build models of cipher devices and to simulate code systems used throughout the United States Government. Computers produce actual cryptographic material for the civil and military agencies of the Government. Computers are the principal intelligence



information handling resource, and also form an integral part of a secure communications system of the United States and its allies.

Much of the automatic data processing resources of the National Security Agency is commercially available, general purpose equipment. In the selection of equipment for application to unique intelligence problems, and in the development of necessary software routines, the National Security Agency produces surveys, analyses, and reports. These documents describe the intelligence problems requiring the acquisition of specific computers, and compare the ability of specific devices to perform the required cryptologic functions. These documents bear the highest authorized national security classifications, and their dissemination is strictly limited and controlled within the National Security Agency and the Government to persons having a need to know for national security purposes.

#### IV. INFORMATION HANDLING AND STORAGE

The missions of the Agency are extremely sensitive in nature, and for that reason, the activities of the Agency and the files relating thereto are compartmentalized. The basic principle of such compartmentalization is to scrupulously restrict access to particular NSA activities and information to

those specific entities or individuals with a legitimate "need to know," and thus to minimize the possible damage to the Agency should a security breach occur. Such compartmentalization is absolutely necessary to ensure the maximum possible protection of the Agency's sensitive activities and information. Depending upon the nature of the particular information in question and its use by the Agency's various components, certain of NSA's "records" are maintained in computerized form. Other NSA records exist only in conventional files which are arranged and indexed according to the particular requirements and needs of the Agency component(s) involved with the materials in question (i.e., the arrangement of such indices varies from component to component). There is no central index to all of the Agency's files. Some files have records in alphabetical order by name, title, or subject matter. Other files are in chronological order; of these, only some, have indexes by name, title or subject matter of the records they contain. There would be an enormous cost for NSA to computerize all of the information in its possession, or to create a single, unified index to all of its records and the contents thereof. In addition, such a comprehensive and unified index of all of NSA's various files and information systems would be both totally unnecessary for the discharge of the Agency's communications security and signals intelligence responsibilities, and dangerously counter-productive to the proper protection of the Agency's uniquely sensitive cryptologic sources and methods.

NSA records fall within four major categories. Three of these categories -- Communications Security (COMSEC), Signals Intelligence (SIGINT), and Research, Development, Test and Evaluation (RDT&E) relate directly to the principal missions of the Agency and are maintained by the organizations under the Deputy Director for Communications Security, Deputy Director for Operations and the Deputy Director for Research and Engineering, respectively. The fourth major category -- administrative and management -- relates to activities in support of the primary missions of the Agency and are maintained by various divisions under the Deputy Director for Administration and miscellaneous specialty divisions.

a. Communications Security (COMSEC) files. These files contain records on matters pertaining to safeguarding United States wire and radio communications, to the production, distribution and control of cryptographic materials, and to the evaluation of cryptographic security regulations.

b. Signals Intelligence (SIGINT) files: These files encompass signals intelligence products, technical reports and related records created as the result of individual and collective analytic reporting activities and collections of

documents or of information of use to Agency analysts generally.

c. Research, Development, Test and Evaluation (RDT&E) files. These files contain records maintained within NSA to support the United States RDT&E effort for COMSEC and SIGINT. Functions included in such support are analytic, communications security and intercept equipment development; engineering, mathematical and physical research; and inspection tests and evaluation of equipments and material.

d. Administrative and Management Files. This category consists of general administrative files; policy and planning files; program/budget files; finance and accounting files; civilian and military personnel files; physical and personnel security files; manpower, paperwork, organization, and committee management files; and files pertaining to publication, printing and reproduction facilities, communications services and various housekeeping functions common to federal agencies.

Records deemed to have no current application are boxed by the Agency organization that is retiring the records and sent to a storage area maintained by the NSA/CSS Records Center. Affixed to each box is a label that includes a description, usually in very general terms, of the contents of the box. The same description is included on a 5" x 8" control card that

records the whereabouts of the box in storage. The means of identifying the contents of the boxes vary from component to component and, among those sent by a particular component, from box to box, depending upon the type of Agency function or activity to which the records within the boxes relate. Thus, records relating to personnel matters are likely to be indexed by individual's names. Records resulting from or relating to the production of communications intelligence functions and activities are likely to be identified by series (roughly chronologically), pertaining, in some cases, to records grouped by geographical area or by broadly defined categories of information. Thus, NSA does have the capacity to retrieve information located in warehouse storage, but -- again barring manual examination of all such records -- retrieval is dependent upon the means for labeling the contents of boxes that are peculiarly adapted to the use to which such records are put, or the happenstance knowledge that a specific document contains the information sought.

The NSA does assign distinctive numbers to individual SIGINT documents. Many of the conventional files possessed by NSA contain documents which have been assigned individual serials, such numbers facilitating reference to a specific document. Beyond its existing indices, NSA has no master list or index correlating individual serials with specific subject

matters or the contents of a given signals intelligence document. Thus, if a search of NSA's existing computerized records and indices to files for particular materials produces negative results, the only additional way to ascertain the existence and location of such materials (other than through a manual search of all of the Agency's records) would be through the happenstance knowledge that a particular serial or serials contain information responsive to the request.

SIGINT files -- At the outset, it must be kept clearly in mind that the NSA is a producer of raw intelligence information, not a producer of finished intelligence. Whereas other agencies compile information from various intelligence sources for evaluation and amalgamation as finished intelligence on particular subjects (such as persons, organizations, installations or events), NSA only gathers intelligence information through signals intelligence processes. Accordingly, NSA does not structure or index its SIGINT files in a manner which would enable the Agency to amass items of intelligence information about particular subjects, but, rather, organizes the files in a way that facilitates the gathering process. Some of the SIGINT files have specialized purposes and others have generalized application. The files maintained by operational components for their own use are structured in ways that permit amassing information about the targeted signals

assigned to them. SIGINT files maintained for general, Agency-wide use, are arranged by producing organization, security classification and report serial number. This system of organizing the general, Agency-wide files is used both in the computer filing system and in the hard copy, paper, files which antedated computer storage of SIGINT and which, in some cases, are still being used.

Administrative and Management Files - Effective 27

September 1975 the administrative and management files of the Agency maintained or indexed by individual names or personal identifiers were established as the NSA Systems of Records under the Privacy Act of 1974. The latest descriptions of the NSA systems of records as required under 5 U.S.C. 552a(e) (4) were published on 18 January 1982. 47 Fed. Reg. 2617 to 2626 (1982). The NSA Systems of Records consist of GNSA01 (NSA/CSS Access, Authority and Release of Information), GNSA02 (NSA/CSS Applicants), GNSA03 (NSA/CSS Correspondence, Cases, Complaints, Visitors, Requests), GNSA04 (NSA/CSS Cryptologic Reserve Mobilization Designee List), GNSA05 (NSA/CSS Equal Employment Opportunity Data), GNSA06 (NSA/CSS Health, Medical and Safety Files), GNSA07 (NSA/CSS Motor Vehicles and Car Pools), GNSA08 (NSA/CSS Payroll and Claims), GNSA09 (NSA/CSS Personnel File), GNSA10 (NSA/CSS Personnel Security File), GNSA11 (NSA/CSS Time, Attendance and Absence), GNSA12 (NSA/CSS Training), and GNSA13

(NSA/CSS Archival Records). Of these systems of records the three systems which would contain references to the records of all persons on whom a record is maintained in the NSA systems of records, i.e., GNSA02, Applicants, GNSA09, Personnel File, and GNSA10, Personnel Security Files, if such records exist, are maintained by the Personnel and Security Offices within the Administration Directorate.

a. The Security Office maintains that system of records, GNSA10 (NSA/CSS Personnel Security File), pertaining to the security background checks and clearance status of individuals given access to NSA information and/or facilities. The Security Office maintains all such files for a minimum period of 15 years after the individual no longer has access. Files would be maintained for a longer period if the individual's access had been removed for cause or the person's clearance were called into question for some reason. When it is determined that particular files are due to be disposed of the Security Office destroys the files and removes the individual names from that office's master listing. Thus, once files are destroyed there is no master listing of the names of those individuals who had had access to NSA information and/or facilities.



b. The Personnel Office maintains those systems of records, GNSA02 (NSA/CSS Applicants) and GNSA09 (NSA/CSS Personnel Files), pertinent to all persons who had either applied for, or been employed, assigned or detailed in positions with the NSA. The files are maintained in various sub-files each of which has its own listing of the individuals within that category. Although the Personnel Office maintains no master list of individuals affiliated with the NSA, past and present, a check of the various sub-files would yield the name of an individual who had been assigned, detailed or employed in NSA and where the individual file is located if not at the NSA. The list of names of employees has been maintained in a computer since the mid-1960's and, prior to that, was maintained on microfiche.

The files maintained by the Agency with respect to assigned military personnel are not maintained in the Personnel Office, but, rather, in a separate office tasked with administering military assignees. The records maintained by this office are routinely destroyed shortly after a military assignee has left his/her assignment at the Agency. Official service records follow the reassigned military person. Records reflecting the association of the military assignee to the Agency, may, thereafter, only be found in the Security Office files which reflect each military assignee's access to NSA information and/or facilities.

In addition to the aforementioned systems of records the Administrative and Management files also consist of those files of the various non-operational, special subject matter divisions which are both name retrievable and non-name retrievable. These files are as many and varied as the individual divisions require them to be as they determine what information should be retained. Accordingly, for example, the Legislative Affairs office might have information relative to legislative hearings and the General Counsel's Office would have information relative to administration of legal matters.

~~TOP SECRET~~

AFSA-008/jew

30 August 1950

~~TOP SECRET~~

MEMORANDUM FOR DIRAFSA:

SUBJECT: Shamrock Operations

1. The attached report is forwarded for your information. With respect to the statement made in paragraph 4, subpara (b), it should be noted that assurances of protection have never been given to the seaman carriers by the Attorney General.

2. Although in certain respects it may be desirable, from a security point of view, to carry on the Shamrock operations in the manner in which it is now done, it entails delays that are not in the best interests of National Security and which were of the greatest consequence in connection with the Pearl Harbor attack. The Pearl Harbor Investigating Committee, in its report, recommended as follows:

"That effective steps be taken to insure that statutory or other restrictions do not operate to the benefit of an enemy or other forces inimical to the Nation's security and to the handicapping of our own intelligence agencies. With this in mind, the Congress should give serious study to, among other things, the Communications Act of 1934."

3. For some time the Department of Defense has been endeavoring to sponsor legislation which would implement the foregoing recommendation. On 4 May 1948, the Chairman of USCIB wrote a letter to Mr. Larkin, of the Office of the Secretary of Defense, expressing the keen interest of USCIB and its member department and agencies in the progress of a proposed bill to amend section 805 of the Communication Act of 1934, and pointing out that it represented an effort to carry out one of the important recommendations of the Pearl Harbor Investigating Committee. Although a bill has been introduced in the House, as far as I know it has progressed no farther than the Committee on Interstate and Foreign Commerce.

4. In view of the crisis that is now confronting us and the emphasis that is being laid upon intelligence, as well as the legal recognition of COMINT Activities implicit in Public Law 518, this would appear to be a propitious time for obtaining passage of the legislation recommended by the Pearl Harbor Investigating Committee.

Approved for Release by NSA on  
05-07-2004, FOIA Case # 43104

~~TOP SECRET~~

*May  
File  
(11-21-50)*

~~TOP SECRET~~

AFSA-00B/jow

~~TOP SECRET~~

20 August 1950

SUBJECT: Sharecropping Operations

\*\*\*\*\*

It would appear to me that it would be desirable for USCIB to get itself on record again and take whatever action might appear appropriate under the circumstances toward accomplishing the end in view. It is suggested that you make such a recommendation to the Board at its next meeting.

J.N. WENGER  
AFSA-00B

Copy furnished:  
AFSA-02

~~TOP SECRET~~

T  
B V 19 K  
19 V B K  
SET 144 RPT 144 SW KC

~~TOP SECRET~~

TO CAPT MASON  
FROM CAPT WENGER

*NO B has been  
advised*

PLEASE GIVE ME ~~THE~~ AVERAGE DELAYS IN RECEIPT OF TRAFFIC FROM  
THE VARIOUS SHAMROCK SOURCES K

RECD AFSA-02 1100 30 AUG 50 K  
SECURING OK

dc ~~xxxx~~  
f.c.e  
lower cut

R/Sut

XXXX/ SET 121 RPT 121 SW KC  
AD K

~~TOP SECRET~~

00

OK JUST A SEC K  
KKKKK

*I have investigated this in  
or, also in State and CIA.  
Cris (Cray and Polygraphics). Results  
are negative. Cray thinks  
information may have come  
from Dept of Commerce which  
has been keeping a close*

TO CAPTAIN WENGER (EYES ONLY)  
FROM CAPTAIN MASON

RE YOUR RECENT EYES ONLY ON SUBJECT OF [REDACTED] VISIT.  
WE HAVE NOT PUBLISHED SUCH A MESSAGE, AND HAVE BEEN UNABLE TO  
LOCATE ANYTHING LIKE IT IN OUR UNPROCESSED MATERIALS. I RATHER  
THINK THAT IF THE INCIDENT DEALS WITH SPECIFIC KNOWLEDGE OF A  
SPECIFIC MESSAGE, I AM INCLINED TO THINK THAT WE ARE NOT THE  
GOVERNMENT AGENCY INVOLVED. THE CHARGE, HOWEVER, MAY BE A  
BLANKET ONE.

(b) (6)

(b) (1)  
(b) (3) - P.L. 86-36

THAT S ALL K  
SECURIN C  
SECURING K

*watched on [REDACTED] but  
has not had any access to  
our material.*

*Shamrock*

Approved for Release by NSA on  
05-15-2014 FOIA Case # 70768

~~TOP SECRET~~

April 26, 1976

*Be  
file*

MEMORANDUM FOR THE RECORD

Of the documents discovered in the National Archives relating to SHAMROCK, the 25 November 1947 memorandum and the 13 December 1947 memorandum are newly discovered records. A copy of the 16 December 1947 memorandum is already in the SHAMROCK files made available to the Senate Select Committee. The 12 November 1947 memorandum is a CIA document, and Jim Nash, on my instructions, has asked the National Archives to send this document to CIA for a determination as to whether it can be declassified.

The unsigned receipt of May 13, 1951 listing seven documents has also been checked against our existing SHAMROCK files. Item 4 on the list, the May 16, 1949 memorandum, is the only document that has not been found.

Mr. S. A. Tucker will check out the whereabouts of the May 16, 1949 memorandum and will recheck the records of the National Archives. His search of Secretary of Defense Johnson's special files produced negative results. He is also having a search conducted at the U.S. Naval Communications Station (because it was listed in the unsigned 1951 receipt) and with Army Chief of Staff (Intelligence), through Mr. Kearney, Deputy General Counsel.

Jim Johnston, Senate Select Committee's Staff Member, has been advised and will inform Fritz Schwartz and Bill Miller that one or more new documents on SHAMROCK have been discovered in the last few days. After Tucker reports back, and after NSA makes a further check, I will invite the Senate Select Committee staff to review all newly discovered papers. Tom Latimer has been advised.

*Robert T. Andrews*

Robert T. Andrews

27 Apr 1976  
DA

(b) (3) - P. L. 86-36

Approved for Release by NSA on 05-07-2004, FOIA Case # 43104



MEMO ROUTING SLIP		NEVER USE FOR APPROVALS, CONCURRENCES, OR SIMILAR ACTIONS	
1	NAME OR TITLE <i>POA</i>	INITIALS <i>AK</i>	CIRCULATE
	ORGANIZATION AND LOCATION	DATE	COORDINATION
2	<i>12</i>		FILE
			INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE
REMARKS <p><i>Capt. Roeder of ONI provides me with three plans for cable &amp; radio collaboration. As they will affect our Shamrock operations we should take note of them and make necessary arrangements with the cognizant officers in ONI. I understand that a code is being under</i></p>			
FROM NAME OR TITLE <i>POA Coey</i>		DATE <i>9/14/51</i>	
ORGANIZATION AND LOCATION <del>CONFIDENTIAL</del>		TELEPHONE	

Approved for Release by NSA on 05-07-2004, FOIA Case # 43104

"Capt Hyland is <sup>the</sup> responsible officer  
to me. Capt Roeder  
has advised on making  
contact."



~~CONFIDENTIAL~~

5 NOV 75

~~SENSITIVE~~

If SHAMROCK disclosure is necessary it might be put in at this point.

Details of our sources of communication are necessarily important to be kept secret from foreign governments since they will certainly take advantage of such knowledge. However, it is unfortunately true that one source has been revealed recently. That is, for many years beginning prior to Pearl Harbor, under certain conditions certain U.S. companies which provide overseas communications permitted the government to have access to selected communications for the purpose of foreign intelligence. These arrangements were very important to the nation and the patriotic citizens who cooperated with their government did so without recompense or favor. These arrangements have now been terminated. The exposure of this activity has impaired this nation's ability to derive foreign intelligence of great value and may well have resulted in injury to cooperating Americans whose only motive was patriotism.

Approved for Release by NSA on  
05-07-2004, FOIA Case # 43104

IV-7 (a)

~~CONFIDENTIAL~~

FSS

18 November 1975

TO: D6, Mr. Banner  
D4, [redacted]

(b) (3) - P.L. 86-36

SUBJECT: Observations on SHAMROCK

The inclosed is forwarded for your information.

*fo*

[redacted]

Approved for Release by NSA on  
05-07-2004, FOIA Case # 43104

November 12, 1975

**MEMORANDUM**

**OFFICE OF THE GENERAL COUNSEL**

Note to

NSA

(b) (3) - P.L. 86-36

I believe you would wish to consider the accompanying November 12 memorandum dealing with the upcoming Friday hearings on Shamrock.

*Robert T. Anderson*

~~Robert T. Anderson~~  
Senior Advisor to the General Counsel

Attachment

*Handwritten signature and initials*  
Cl?  
?



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE  
WASHINGTON, D. C. 20301

November 12, 1975

COMPTON

MEMORANDUM FOR Mr. Robert T. Andrews  
Office of General Counsel

SUBJECT: Observations on Shamrock Report

*BW*  
I have reviewed the package you furnished comprised of S. RES. 21, a resolution in the Senate to establish the Church Committee, the Rules of Procedure for the Committee and the October 29, 1975 paper on Operation Shamrock.

From S. RES. 21, it appears that Section 7 on page 11 provides for the Committee to establish its own rules and procedures to prevent the disclosure of classified information outside the Committee. Implicit in this is the provision that the Committee may also establish rules and procedures to disclose such information.

Section 7.5 of Rule 7 of the Committee's Rules on Procedures provide that classified information may be disclosed outside the Committee only by a majority vote of the entire Committee.

The question arises whether the Senate or the House derives authority from the Constitution to declassify information classified by the Executive Branch. I don't believe that we should admit openly that the effect of the Committee's vote was to declassify the information contained in the 7 page document on Operation Shamrock since, in my view, declassification action can only be taken under the authority of E. O. 11652. Rather, we should take the view that the Committee "disclosed" the information and, in light of that disclosure and the fact that Operation Shamrock was terminated by the Secretary of Defense in May 1975, the information will be reviewed for possible declassification as is our practice with any other disclosure of classified information.

To only admit that the public disclosure of the information contained in the 7 page document by the Committee effectively declassified the



compromise

information may be the beginning of a "revelation race" between Committees. By this I mean that the House Committee might be provoked to "reveal" more information on Operation Shamrock or other ongoing classified operations by the knowledge that such action brings about automatic declassification on the part of the Executive Branch.

At some point, the line should be held. There may be merit to the following approach. General Allen could propose that his testimony be given in executive session. He could explain that under the provisions of the National Security Act of 1947 cognizance is taken of the legitimacy of the need to protect intelligence sources and methods. One means of protection is the classification system provided by E. O. 11652. Certainly any classified information which is supplemental to that disclosed by the Church Committee relating to Operation Shamrock or other ongoing operations of the Agency which involve sources and methods does continue to qualify for security classification protection under E.O. 11652. In addition, General Allen could advise the Committee that information concerning the organization, functions and activities of his Agency may be withheld from public disclosure under PL 86-36 and further that such information may be withheld, in turn, under the Freedom of Information Act. Testifying on activities of his Agency in open session is tantamount to public release.

The precise information disclosed by the Church Committee which concerns Operation Shamrock (and any related information now held classified by the National Security Agency) should, in light of the "disclosure" and the fact that Shamrock has been terminated, be reviewed to determine whether downgrading or declassification is warranted. Such action is required by the provisions of Section 2-312, DoD ISPR 5200.1-R. Pending that determination "by a competent Government authority," however, the classified information which was "disclosed" remains classified.



Arthur F. Van Cook  
Director of Information Security  
ODASD(Security Policy)

Background  
Shamrock Report

FOR IMMEDIATE RELEASE

NOVEMBER 6, 1975

Office of the White House Press Secretary

THE WHITE HOUSE

## STATEMENT BY THE PRESS SECRETARY

The President regrets that the Senate Select Committee has publicly discussed the activity known as "Operation SHAMROCK", which was instituted over 25 years ago by President Truman, his Secretary of Defense and Attorney General. Although this was terminated in the Spring of this year because of allegations that portions of the National Security Agency activity were improper, the President has refrained from discussing this publicly in order to avoid any criticism or any implied criticism of former officials who acted in good faith during difficult times in the cold war period and to protect legitimate on-going foreign intelligence activity by the National Security Agency.

Instead, the President has endeavored to make all the information concerning SHAMROCK available to the Senate Select Committee and the Department of Justice in order to assure that appropriate legislation can be developed, if necessary, and the Attorney General can conduct his investigations. The President has tried to act responsibly by taking effective actions to stop possible abuses and prevent any recurrence without seeking publicity when the activity was terminated.

There are two critically important objectives concerning the intelligence community investigations:

1. We must develop the appropriate facts so that legislation, if necessary, can be enacted and any legal action, if warranted, can go forward.
2. We must do this in a manner which does not unnecessarily damage our foreign intelligence capabilities.

The national interest requires a careful balancing of these two objectives.

All of those who are involved with this matter in an official capacity must take care to permit the investigation to go forward in a reasonable manner without damage to our ability to develop appropriate foreign intelligence.

Approved for Release by NSA on  
05-07-2004, FOIA Case # 43104

SHAMROCK



~~TOP SECRET~~

CAPT MASON FROM CAPT WENGER

(b) (6)

[REDACTED] IS COMING TO SEE ADM STONE AT 1130 FRIDAY 26  
JAN ABOUT A MATTER HAVING TO DO WITH SHAMROCK. PRIOR TO THAT  
TIME PLEASE LET ME HAVE ALL THE DETAILS ABOUT OUR ARRANGEMENTS  
WITH [REDACTED]

WE '23 JAN 1951 JOW K  
R EJR  
SECURING K  
VA

Approved for Release by NSA on  
05-07-2004. FOIA Case # 43104

O-SHAMROCK

~~TOP SECRET~~ ~~U.S. OFFICIALS ONLY~~  
~~CANOE~~

025

~~SECURITY INFORMATION~~

Commercial Messages in Shamrock Material

F 11.

NSA-21

NSA-26

15 Jan 53

1. It is our understanding that at present, NSA-21 forwards only ~~Government~~ plain-text and cipher traffic removed from the subject material.

2. It is requested that NSA-21 investigate the feasibility of also removing commercial traffic for ultimate forwarding to NSA-262, since it is felt that information of value may be derived from this material.

CHARLES H. CONNELLY  
NSA 26A

Approved for Release by NSA on  
03-27-2014, FOIA Case # 70768

~~TOP SECRET~~ ~~CANOE~~ ~~U.S. OFFICIALS ONLY~~