U.S. Department of Homeland Security

United States Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King Ave SE
STOP 7301
WASHINGTON DC 20593-7301
Staff Symbol: CG-2
Phone: (202) 372-2601
Fax: (202) 372-2312

5720
FOIA 2014-2799

Alan Butler, EPIC Appellate Advocacy Council
Ginger McCall, Director, EPIC Open Government Project
1718 Connecticut Ave NW
Suite 200
Washington DC 20009

Dear Mr. Butler and Ms. McCall:

This is the final response to your 31 July 2014, Freedom of Information Act (FOIA) request to the U.S. Coast Guard (USCG) for "records related to the government's surveillance and collection of electronic communications outside the United States under Executive Order 12333 ("EO 12333"), and other related Executive Orders, including the collection and interception of messages, metadata, and other transactional and business records regarding e-mail, telephone, and Internet usage". This office received your request on 15 September 2014.

In responding to a FOIA request, the USCG will search for responsive documents in its control on the date the search began. We began our search on 15 September 2014.

We are granting your request under the FOIA, Title 5 U.S.C. § 552, as amended, and DHS' implementing regulations, 6 C.F.R. Chapter I and Part 5. After carefully reviewing the responsive document: Commandant Instruction M3820.12, Coast Guard Intelligence Activities, Procedure 5, I determined that it is appropriate for public release. They are enclosed in their entirety; no deletions or exemptions have been claimed.

Provisions of the FOIA allow us to recover part of the cost of complying with your request. In this instance, because the cost is below the $14 minimum, there is no charge.

If you need to contact us about this request, please refer to **2014-2799**. You may contact this office at (202) 372-2714.

Sincerely,

Mr. Daniel Butler
Deputy, Assistant Commandant for
Intelligence and Criminal Investigations

Enclosure: Commandant Instruction M3820.12,
Coast Guard Intelligence Activities, Procedure 5 (3 pages)

PROCEDURE 5

ELECTRONIC SURVEILLANCE FOR INTELLIGENCE PURPOSES

A. Non-consensual Electronic Surveillance Within the United States for Intelligence Purposes.

1. Applicability.

   a. Procedure 5.A implements the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §1801, *et seq.*, and applies to "electronic surveillance," as defined in the FISA, conducted by Coast Guard national intelligence components within the "United States" to collect "foreign intelligence information," as defined in the FISA.

   b. Procedure 5.A applies to all non-consensual "electronic surveillance," as defined in the FISA, conducted within the United States, whether or not directed against USPer, by Coast Guard national intelligence components.

   c. Procedure 5.A does not govern circumstances in which the Federal Bureau of Investigation, National Security Agency, or other authorized agency of the Federal government conduct authorized electronic surveillance under the FISA in response to a Coast Guard request for intelligence support. Only the Assistant Commandant for Intelligence is authorized to submit such requests for intelligence support to the Federal Bureau of Investigation or the National Security Agency.

   d. Procedure 5.A does not apply to authorized electronic surveillance conducted for the primary purpose of law enforcement by law enforcement intelligence or non-intelligence components of the Coast Guard in accordance with applicable law (i.e., Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986, 18 U.S.C. 2510, *et seq.*).

2. Procedures.

   a. Coast Guard national intelligence components shall not conduct non-consensual electronic surveillance within the United States for intelligence purposes unless pursuant to an Order issued by a judge of the court appointed pursuant to the FISA or pursuant to a certification of the Attorney General issued under the authority of section 102(a) of the FISA.

   b. Requests by supervisors of Coast Guard national intelligence components for authority to conduct non-consensual electronic surveillance pursuant to the FISA shall be submitted by secure, expeditious means via the servicing legal office to the Assistant Commandant for Intelligence in manner prescribed by the Assistant Commandant for Intelligence.

B. Non-consensual Electronic Surveillance Outside the United States Against United States Persons for Intelligence Purposes.

1. Applicability.

a. Procedure 5.B applies to non-consensual electronic surveillance, as defined in Enclosure (1), conducted by Coast Guard national intelligence components for intelligence purposes directed against a "United States person," as defined in the FISA, who is *outside the United States*.

(1) Electronic surveillance is "directed against a USPer" when the surveillance is intentionally targeted against or designed to intercept the communications of or concerning that person.

(2) Electronic surveillance directed at non-USPer that results in the "inadvertent acquisition of USPer communications" incidental to authorized collection does not automatically become directed against a USPer.

(3) Electronic surveillance is directed against a USPer who is "outside the United States" if the person against whom the electronic communication is directed is not physically within the United States, regardless of the location at which the surveillance is conducted. For example, if the interception of communications that originate and terminate outside the United States is conducted from within the United States, the provisions of 5.B rather than 5.A apply.

b. Procedure 5.B also governs the non-consensual use of mechanical or other surveillance devices for intelligence purposes by Coast Guard national intelligence components directed at a USPer outside the United States in circumstances where such person has a reasonable expectation of privacy.

2. Procedures.

a. Coast Guard national intelligence components shall not conduct non-consensual electronic surveillance outside the United States directed against a USPer for intelligence purposes unless pursuant to an approval issued by the Attorney General.

b. Requests by supervisors of Coast Guard national intelligence components for authority to conduct electronic surveillance under Procedure 5.B shall be submitted by secure, expeditious means via the servicing legal office to the Assistant Commandant for Intelligence in manner prescribed by the Assistant Commandant for Intelligence.

3. Emergency Situations.

a. The Assistant Commandant for Intelligence is authorized to approve non-consensual electronic surveillance outside the United States directed against a USPer if:

(1) On the basis of facts and circumstances the Assistant Commandant for Intelligence determines there is probable cause to believe that the target of the surveillance is a foreign power or agent of a foreign power; and

(2) Securing approval from the Attorney General is not practical because:

(i) The time required would cause failure or delay in obtaining significant foreign intelligence or counterintelligence and such failure or delay would result in substantial harm to national security; or

(ii) A person's life or physical safety is reasonably believed to be in immediate danger.

b. The Assistant Commandant for Intelligence shall immediately notify the Chief Counsel and the Attorney General as soon as possible of the surveillance, the circumstances surrounding its authorization, the results thereof, and any such other information as may be required to authorize continuation of such surveillance.

c. Electronic surveillance authorized pursuant to Procedure 5.B.3 may not continue beyond the time required for a decision by the Attorney General, and in no event beyond 72 hours.

C. Information Assurance Activities.

1. Applicability. Procedure 5.C applies to the conduct of information assurance activities (e.g., technical surveillance countermeasures, vulnerability surveys, hearability surveys).

2. Procedures. Coast Guard national intelligence components conducting information assurance activities shall comply with policies and procedures promulgated in directives issued by the Director, National Security Agency/Chief, Central Security Service, with the approval of the Attorney General.