Legislative & Regulatory Counsel

22 February 1984

84-0688

STAT

NOTE TO: [redacted]

Deputy Director of Legislative
Liaison
Room 7D43
Central Intelligence Agency

Attached is a copy of comments on H.R. 4620 that we provided to Congressman Brooks at his request.

STAT [redacted]

Encl:
a/s

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755

Serial: N-0272
21 February 1984

The Honorable Jack Brooks
Chairman, Committee on Government Operations
United States House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

The Director, National Security Agency, Lt Gen Lincoln D. Faurer, has asked that I respond to your letter of February 6, 1984, requesting a report and comments on H.R. 4620, the "Federal Telecommunications Privacy Act of 1984."

Summary of the Bill

H.R. 4620 would prohibit federal officers and employees from recording or listening-in upon any conversation conducted on a federal telecommunications system or conducted on any other telecommunications system if the conversation is between a federal officer or employee and any other person and involves the conduct of Government business.

Exempted under subsection (b) would be the recording of, or listening-in upon, a conversation without the consent of any party to it when the recording or listening is authorized under the Omnibus Crime Control and Safe Streets Act of 1968 or the Foreign Intelligence Surveillance Act.

Exempted under subsection (c) would be the recording of, or listening-in upon, a conversation with the consent of one party to it when the recording or listening-in is performed (1) for law enforcement purposes, (2) for counterintelligence purposes, (3) for public safety purposes, (4) by a handicapped employee as a tool necessary to his or her performance of official duties, or (5) for service monitoring purposes.

Recording of or listening-in upon telephone conversations pursuant to subsection (c)(3), (4), and (5) must have prior approval by the agency head or designee of written determinations specifying the operational need for listening-in or recording conversations, the system and location where it is to be performed, the telephone numbers and recorders involved, and operating times and the expiration date and justifying the use. Service monitoring under subsection(c)(5) could be conducted only by designated personnel after positive action to inform callers of the monitoring and labeling of telephone instruments subject to the monitoring. Only the minimum number of calls necessary to compare a statistically valid sample could be monitored. No data identifying the caller could be recorded by the monitoring party, and no

information obtained by the monitoring could be used against the calling party.

Under subsection (d) recording of or listening-in upon a telephone conversation with the consent of all parties to it could be conducted in cases of telephone conferences, secretarial recording, and other acceptable administrative practices under strict supervisory controls to eliminate possible abuses.

Current copies and subsequent changes of agency documentation, determinations, policies, and procedures supporting operations pursuant to subsections (c)(3), (4), or (5) would be required to be forwarded before the operational date for the General Services Administration (GSA). The GSA would be accountable for information concerning operations under subsection (c)(3), (4), and (5), and for periodically reviewing listening-in programs with agencies to ensure compliance with federal property management regulations. The GSA would be charged with obtaining compliance with the enacted H.R. 4620 if an agency failed to document its devices in accordance with the Act.

Subsection (g) provides that any recording or transcription of a conversation made under (or in violation of) the Act would be a record within a system of records under the Privacy Act of 1984 as to each party to the conversation. Subsection (h) would include any such recording or transcription within the protection of a criminal statute prohibiting the concealment, removal, mutilation, obliteration, falsification, or destruction of records filed with officials of U. S. courts or other public office.

Effects on NSA

Set forth below are the effects that this bill would have on the activities of the National Security Agency (NSA). In reviewing these effects, you should keep in mind two key points. First, the bill proposes to legislate in an exceedingly complex area, i.e., electronic surveillance. H.R. 4620 would be at least the fourth statute that affects monitoring of telecommunications (see also 18 U.S.C. §§2510 et seq., 47 U.S.C. §605, and 50 U.S.C. §1801 et seq.). The three existing statutes are not well integrated with each other, and against this background H.R. 4620 inevitably adds complexity. Without more time to consult with all interested parties in the Executive Branch, I cannot be certain that the full impact of H.R. 4620 on NSA is yet recognized. Thus, this Agency may be required to supplement these comments. Second, while the scope of H.R. 4620 as regards the activities of NSA is potentially quite broad, the actual incidence of some effects may be very infrequent. For example, in the conduct of its SIGINT mission NSA rarely, if ever, overhears the telecommunication of

a federal employee discussing Government business. Nevertheless, it is a possibility and could occur accidentally in the course of an overseas surveillance which is not conducted under the Foreign Intelligence Surveillance Act.

Two primary missions of the National Security Agency (NSA) would be affected by your proposed statute. Significant aspects of the Agency's signals intelligence (SIGINT) mission are governed by the Foreign Intelligence Surveillance Act of 1978 (FISA). By virtue of subsection (b), that mission would be unaffected by the Act, unless recordings made under FISA authority would be deemed to be "made under...this Act" and therefore deemed records in a system of records for Privacy Act purposes and records for purposes of the criminal statute cited in subsection (h).

Automatically declaring a SIGINT recording as a Privacy Act record regardless of how the recording is maintained and retrieved would be inappropriate for several reasons. First, statutory minimization procedures require deletion of personal identifiers in many cases. Second, it would be impossible to comply with Privacy Act requirements without creating an index--a process that would be very costly and counterproductive to privacy concerns. Finally, disclosure of the fact alone that a telephone conversation of a particular person had been intercepted and processed for SIGINT purposes by NSA could jeopardize SIGINT sources and methods and would be a fact that the Agency could neither confirm nor deny. The adverse consequences of declaring all recordings made under (or in violation of) this Act to be Privacy Act records also apply, in varying degrees, to the other Agency functions discussed in this letter.

NSA conducts a number of SIGINT activities at the request of federal officials directed against their communications for counterterrorism purposes. Since counterintelligence is not defined, it appears necessary to amend (c)(2) by adding "or counterterrorism" in line 11, page 3, after counterintelligence.

NSA also conducts other SIGINT activities that either intentionally or accidentally could monitor or record communications within the scope of Section 113(a)(2). For example, the Agency or its associated military components may monitor U.S. military exercise communications. Because of the nature of exercises, it is rarely possible to secure consent of any party, let alone all parties to a communication. As mentioned previously, it is also possible that in the course of SIGINT activities conducted outside the scope of FISA incidental overhears are possible. Finally, NSA, or other intelligence agencies, could be authorized by the Attorney General pursuant to E.O. 12333 to conduct electronic surveillance of a federal employee abroad, i.e., outside

the scope of FISA. Such a surveillance could acquire communications within the scope of Section 113(a)(2). These problems could be avoided by adding a new subparagraph to Section 113(b):

> "(3) Without the consent of any party to a conversation, the recording of, or listening-in upon, such conversation may be conducted notwithstanding subsection (a) if such recording or listening is conducted against communications outside the scope of Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. 2510 et seq.) or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), is conducted by an agency in the Intelligence Community, and is conducted pursuant to guidelines approved by the Attorney General."

The second of the Agency's primary missions that would be affected by your proposed statute is communications security (COMSEC). COMSEC means protective measures taken to deny unauthorized persons information derived from telecommunications of the U. S. Government, including certain contractors of the Government, related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including crypto security, transmission security, emissions security) to electrical systems generating, handling, processing, or using national security or national security related information. It also includes the application of physical security measures to COMSEC information or materials. Systematic examinations of telecommunications are carried out to determine the adequacy of COMSEC measures, to identify COMSEC deficiencies, to provide data from which to predict the effectiveness of proposed COMSEC measures, and to confirm the adequacy of such measures after implementation. COMSEC monitoring is an essential part of such examinations, and is conducted pursuant to detailed guidelines approved by the Attorney General. COMSEC monitoring is the act of listening to, copying, or recording transmissions of Executive Branch official telecommunications, including the communications of certain contractors, to provide technical material for analysis in order to determine the degree of cryptographic or transmission security being provided to these transmissions. This monitoring is only infrequently conducted and notice is required to be provided to persons utilizing communications systems subject to such monitoring. COMSEC monitoring must be exempted from the prohibitions in your bill. None of the exemptions included in H.R. 4620 as introduced covers COMSEC monitoring. I propose that the following paragraph be added under subsection (c):

"(6) The recording or listening-in is performed by or under the authorization of the Executive Agent for Communications Security for the purpose of communications security (COMSEC) monitoring to obtain material for analysis in order to determine the adequacy of COMSEC measures, to identify COMSEC deficiencies, to provide data from which to predict the effectiveness of proposed COMSEC measures, and to confirm the adequacy of such measures after implementation. Such monitoring shall be conducted pursuant to guidelines approved by the Attorney General."

NSA is also authorized to monitor and record communications to train its personnel and to test its equipment. To protect private citizens from such activities a preferred target for such monitoring is Government telecommunications. While existing procedures also state a preference for consensual monitoring, it is rarely possible to assure that all parties to these communications consent. While the FISA authorizes monitoring for these purposes the scope of FISA is much narrower than the scope of H.R. 4620. FISA only affects monitoring which constitutes electronic surveillance as defined in 50 U.S.C. 1801(f)(1)-(4), i.e., in general terms, electronic surveillance in the United States. H.R. 4620 would also affect monitoring which occurred abroad. To avoid the unintended impact of the unequal scope of these statutes, I propose the following paragraph be added under subsection (b) after inserting "(1)" after "(b)":

"(2) Without the consent of any party to a conversation the recording or listening-in may be performed notwithstanding subsection (a) by a federal agency to train personnel in the use of electronic surveillance equipment or to test the capability of electronic equipment. The Attorney General shall approve procedures for such recording or listening-in consistent with the criteria and limitations of 50 U.S.C. 1805(f)(1) and (3)."

Recording or listening-in is performed by NSA employees for public safety and service monitoring purposes on telecommunications systems used at NSA to support SIGINT and COMSEC operations. The recordings resulting from such monitoring often contain highly classified information or information that, even if unclassified, may be withheld from disclosure by the Agency under section 6 of the National Security Agency Act of 1959, as amended. 50 U.S.C §402 (note). Subsection (e)(2) of H.R. 4620 should be amended by adding after "subsection (c)" on line 8, page 6, the following clause:

"except such operations conducted to support the activities of the National Security Agency."

Serial: N-0272

Representatives of the National Security Agency would, of course, be pleased to meet with you to discuss the concerns set forth above. My telephone number is 688-6705.

Sincerely,

STAT

[redacted]

General Counsel