

20 NOVEMBER 1977

PAB - 3

# U.S. Businesses Warned of Soviet Eavesdropping

By CHARLES OSOLIN

Special-Contributor Washington Bureau

WASHINGTON — The Carter administration is warning the U.S. business community to avoid discussing sensitive technological or

economic information over the telephone because it may be overheard by Soviet agents and industrial spies.

In a major break with the secrecy that has surrounded electronic eavesdropping in

the past, administration officials are alerting major defense contractors and other industries that their telephone calls are being or could be intercepted by spies using sophisticated electronic equipment.

According to government officials familiar with the briefings, industry executives are being told that their long-distance phone calls are being overheard as they are relayed either by ground microwave links or by domestic communication satellites.

The companies that operate the telephone circuits also are being alerted to the danger.

The officials said the first briefings are being given to companies which are either known to be targets of Soviet microwave eavesdropping or which are "possible" targets because of the nature of their business and the routing of their telephone calls.

The warnings are focusing on companies using private, or leased, telephone circuits, because they are the most vulnerable to electronic eavesdropping.

The officials said the government has no direct evidence that the Soviets are listening in on the commercial long distance microwave network used by most Americans, although such monitoring is technically possible.

The officials confirmed previous disclosures that Soviet agents at four microwave eavesdropping sites in three U.S. cities have been tuning in on government and private microwave transmissions for several years.

According to intelligence sources, the phone calls are being picked up by sensitive antennas on the roof of the Soviet Embassy in Washington, the Soviet Union's mission to the United Nations and its diplomatic retreat in New York City, and at its consulate in San Francisco.

Soviet spy ships anchored off the U.S. coast, as well as "ferret" satellites orbiting overhead, are also thought to be intercepting microwave transmissions.

Intelligence sources have said the Pentagon's National Security Agency became aware of the Soviet eavesdropping several years ago and launched a top-secret project to counter it.

The effort was ordered continued by President Carter in March, and the industry briefings began this summer while the White House was developing a comprehensive plan to deal with the problem.

Eleven communications firms and 17 industrial and commercial businesses had been briefed by the end of last week.

In addition to the industry briefings, officials said the United States is "discussing" the eavesdropping as part of its continuing negotiations with the Soviet Union to halt the sporadic microwave bombardment of the U.S. Embassy in Moscow.

The microwave "flooding" of the embassy, which some medical experts believe has adversely affected the health of State Department officials working there, is thought to be an attempt by the Soviets to jam U.S. microwave monitoring equipment similar to

Sources have said that one reason the U.S. government has been so reluctant to discuss publicly the Soviet interception of domestic phone calls in the United States was the fear that it would endanger the U.S. security agency's worldwide eavesdropping programs in Russia and other countries.

Sen. Daniel P. Moynihan, D-N.Y., a member of the Senate Intelligence Committee who has blasted the Carter administration for allowing the eavesdropping to continue without protest, said Friday that the effort to "alert the American people" to the problem was "responsible and laudable."

Moynihan, who has introduced legislation that would require the U.S. to eject any foreign diplomat caught eavesdropping on the U.S. telephone system, also praised the decision to "raise this matter in negotiations with the Soviet Union. They (the Soviets) may indeed find it strange that we worry so much about protecting the privacy of our citizens. But that is their problem, not ours."

Government officials said the Soviet eavesdropping does not pose a significant threat to classified defense information, since that is always transmitted in code or on "secure" communications links. But they noted that a large amount of unclassified data, such as technological developments and "inside" economic information, could be collected and used by foreign agents against the best interests of the United States.

They also noted that such

information could be used by industrial spies to gain an economic advantage over their competitors, and warned that the same technology that enables the Soviets to monitor microwave links is also readily available to private citizens in the United States.

The officials said the Soviets apparently are focusing

their monitoring effort on leased circuits because calls from a particular company or individual are always routed along the same circuit, and because it is easier for computers to sort through the calls on such circuits and locate information of interest.

On the regular long distance commercial network, calls are relayed along a variety of routes — using cables as well as microwave and satellite relays — making it extremely difficult, if not impossible, to locate all calls from a particular telephone or company at a single monitoring site.

Officials said President Carter last week approved a number of additional government initiatives to counter the Soviet eavesdropping threat. Among them were:

- Creation of a 12-member White House committee, headed by Carter's adviser on

CONTINUED

science and technology, Dr. Frank Press, to coordinate the efforts of the Defense and Commerce departments and other agencies attempting to improve telephone security.

- Increasing the government's research and development budget for communications security equipment from \$10 million during the current fiscal year to \$15 million for FY 1978.

- Rerouting most government calls in Washington, New York and San Francisco from microwave to cable, to eliminate the possibility of Soviet monitoring. The rerouting project has nearly been completed in Washington, and should be finished in New York and San Francisco by the end of next year.

- Continuing the development of an "executive secure voice network" system, which allows government officials to make telephone calls on regular commercial or govern-

*Soviet spy ships anchored off the U.S. coast, as well as orbiting satellites, are also thought to be intercepting microwave transmissions.*

ment lines. The system, developed by the security agency, is linked to a central computer which encrypts the voice signals at one end and decrypts them at the other, and it currently in use in about 100 government offices. Although the "pilot" equipment now costs about \$35,000 for each unit, officials said the government has ordered

150 more units at about \$5,000 apiece.

- Testing, early next year, a new device that would spread the telephone signal on a microwave circuit over a much wider bandwidth than is used in current equipment, making it more difficult to intercept.

- Working with commercial telephone companies to

develop new microwave and communications technology that will make it easier for telephone users desiring privacy to encrypt their telephone calls and computer data transmissions, and more difficult for would-be eavesdroppers to locate calls from a particular telephone.

- Promoting use of a data encryption key that can be used to encrypt computer data before it is transmitted by commercial communications links. The key, developed by the Commerce Department, is now commercially available for only \$15.