U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

July 14, 2015

The Honorable Charles E. Grassley
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

This responds to your letter to Deputy Attorney General Sally Quillian Yates, dated April 27, 2015, concerning the Drug Enforcement Administration's (DEA) purchase and overseas use of commercially-available software to collect data on foreign-based, non-U.S. person criminal targets, as well as DEA's corresponding policies and procedures. DEA has provided the following information in response to your letter. We apologize for our delay in responding.

The Department is committed to using all law enforcement resources in a manner that is consistent with the requirements and protections of the Constitution and other legal authorities, and with appropriate respect for privacy and civil liberties. We are likewise committed to ensuring that the Department's practices are lawful and respect the important privacy interests of the American people.

In 2012, having encountered evidence collection challenges in a number of foreign investigations, and without the resources to internally develop its own technical solution, DEA sought to lawfully acquire a commercially-available tool that would allow for remote, overseas deployment of communication monitoring software on foreign-based devices used by foreign-based drug traffickers and money launderers. DEA evaluated products from a number of companies offering such technology and ultimately determined that commercially-available software named Da Vinci Remote Control System (RCS) was the most secure and capable tool suited for DEA's needs.

As advertised and tested, the RCS software can be remotely deployed on a device, as well as installed through physical access. Once deployed, the software facilitates access to data on the device, including communications and location information. RCS is the only tool or software that DEA has purchased for this purpose. DEA has spent approximately $927,000 on RCS (including on the technology and associated training). Although the licensing agreement extends to the end of Calendar Year 2015, DEA recently elected to cancel its contract.

DEA has only deployed RCS in one foreign country and did so pursuant to foreign court authorization (*i.e.*, judicial wiretap orders), with the foreign host country government's cooperation, and with tight access and use restrictions, as further delineated below. All of the targeted devices' users are foreign-based, non-U.S. persons of mutual investigative interest to both DEA and the foreign host country. The foreign host country already had open criminal investigations on each target prior to RCS's deployment on their devices. The foreign host country selected the devices to be targeted because conventional network intercept methods were either unavailable or unworkable, and a foreign host country prosecutor obtained the authorizing wiretap orders.

Since DEA began this initiative in 2012, RCS has been deployed on 17 devices, which were provided to 17 foreign-based drug traffickers and money launderers pursuant to foreign court orders. Because of technical difficulties with the software, there has only been one successful instance of remote deployment, and it was under controlled circumstances (*i.e.*, a foreign-based cooperating source had access to the targeted device and was able to facilitate installation). The remaining 16 deployments occurred through direct physical access to the targeted devices, with a foreign-based cooperating source then providing the devices to the targeted foreign-based drug traffickers and money launderers. Further, RCS has only been used to collect real-time written communications (*i.e.*, chat sessions and text messages) and location information of the foreign-based drug traffickers and money launderers.

RCS is stored in a secure, DEA-controlled and maintained section within a vetted facility in the foreign host country. DEA restricts physical and system access to RCS—including for configuration and deployment—to designated, trained U.S.-person DEA personnel located in the foreign host country. Those personnel have authority to deploy and terminate interception facilitated by RCS in accordance with the authorized foreign judicial order. Foreign host country personnel do not have unfettered access to RCS. Rather, they provide the targeted devices to the U.S.-person DEA personnel located in the foreign host country, who, in turn, install the RCS software on the devices and then return the devices to the foreign host country personnel to be given to the foreign-based drug traffickers and money launderers.

The collected data is securely transmitted to the foreign host country facility and stored at that location on a server maintained by DEA. The collected data cannot be accessed remotely from the United States. Vetted foreign law enforcement officers, as well as co-located DEA officers working with them, have access to the collected data for official investigative and evidentiary purposes.

The RCS administrator is a trained U.S.-person DEA employee working in the foreign host country and receives system notifications regarding the use of RCS to safeguard against unauthorized use. All access, configurations, and use of RCS are administratively logged in a system maintained by DEA in the foreign host country, with no remote access from the United States. U.S.-person DEA personnel located in the foreign host country run system checks on RCS to ensure it is only deployed on authorized foreign-based targets. At all times, DEA maintains

control of RCS, and DEA has the ability to unilaterally terminate deployment, including on in-use devices. DEA is not aware of any instances of misconduct or misuse relating to the deployment of RCS.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

Peter J. Kadzik
Assistant Attorney General

cc: The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

July 14, 2015

The Honorable Charles E. Grassley
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

This responds to your letter to Deputy Attorney General Sally Quillian Yates, dated April 27, 2015, concerning the Drug Enforcement Administration's (DEA) purchase and overseas use of commercially-available software to collect data on foreign-based, non-U.S. person criminal targets, as well as DEA's corresponding policies and procedures. DEA has provided the following information in response to your letter. We apologize for our delay in responding.

The Department is committed to using all law enforcement resources in a manner that is consistent with the requirements and protections of the Constitution and other legal authorities, and with appropriate respect for privacy and civil liberties. We are likewise committed to ensuring that the Department's practices are lawful and respect the important privacy interests of the American people.

In 2012, having encountered evidence collection challenges in a number of foreign investigations, and without the resources to internally develop its own technical solution, DEA sought to lawfully acquire a commercially-available tool that would allow for remote, overseas deployment of communication monitoring software on foreign-based devices used by foreign-based drug traffickers and money launderers. DEA evaluated products from a number of companies offering such technology and ultimately determined that commercially-available software named Da Vinci Remote Control System (RCS) was the most secure and capable tool suited for DEA's needs.

As advertised and tested, the RCS software can be remotely deployed on a device, as well as installed through physical access. Once deployed, the software facilitates access to data on the device, including communications and location information. RCS is the only tool or software that DEA has purchased for this purpose. DEA has spent approximately $927,000 on RCS (including on the technology and associated training). Although the licensing agreement extends to the end of Calendar Year 2015, DEA recently elected to cancel its contract.

DEA has only deployed RCS in one foreign country and did so pursuant to foreign court authorization (*i.e.*, judicial wiretap orders), with the foreign host country government's cooperation, and with tight access and use restrictions, as further delineated below. All of the targeted devices' users are foreign-based, non-U.S. persons of mutual investigative interest to both DEA and the foreign host country. The foreign host country already had open criminal investigations on each target prior to RCS's deployment on their devices. The foreign host country selected the devices to be targeted because conventional network intercept methods were either unavailable or unworkable, and a foreign host country prosecutor obtained the authorizing wiretap orders.

Since DEA began this initiative in 2012, RCS has been deployed on 17 devices, which were provided to 17 foreign-based drug traffickers and money launderers pursuant to foreign court orders. Because of technical difficulties with the software, there has only been one successful instance of remote deployment, and it was under controlled circumstances (*i.e.*, a foreign-based cooperating source had access to the targeted device and was able to facilitate installation). The remaining 16 deployments occurred through direct physical access to the targeted devices, with a foreign-based cooperating source then providing the devices to the targeted foreign-based drug traffickers and money launderers. Further, RCS has only been used to collect real-time written communications (*i.e.*, chat sessions and text messages) and location information of the foreign-based drug traffickers and money launderers.

RCS is stored in a secure, DEA-controlled and maintained section within a vetted facility in the foreign host country. DEA restricts physical and system access to RCS—including for configuration and deployment—to designated, trained U.S.-person DEA personnel located in the foreign host country. Those personnel have authority to deploy and terminate interception facilitated by RCS in accordance with the authorized foreign judicial order. Foreign host country personnel do not have unfettered access to RCS. Rather, they provide the targeted devices to the U.S.-person DEA personnel located in the foreign host country, who, in turn, install the RCS software on the devices and then return the devices to the foreign host country personnel to be given to the foreign-based drug traffickers and money launderers.

The collected data is securely transmitted to the foreign host country facility and stored at that location on a server maintained by DEA. The collected data cannot be accessed remotely from the United States. Vetted foreign law enforcement officers, as well as co-located DEA officers working with them, have access to the collected data for official investigative and evidentiary purposes.

The RCS administrator is a trained U.S.-person DEA employee working in the foreign host country and receives system notifications regarding the use of RCS to safeguard against unauthorized use. All access, configurations, and use of RCS are administratively logged in a system maintained by DEA in the foreign host country, with no remote access from the United States. U.S.-person DEA personnel located in the foreign host country run system checks on RCS to ensure it is only deployed on authorized foreign-based targets. At all times, DEA maintains

control of RCS, and DEA has the ability to unilaterally terminate deployment, including on in-use devices. DEA is not aware of any instances of misconduct or misuse relating to the deployment of RCS.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

Peter J. Kadzik
Assistant Attorney General

cc: The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu