NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
OFFICE OF THE INSPECTOR GENERAL

11 September 2013

Sen. Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
152 Dirksen Senate Office Building
Washington, DC 20510

Senator Grassley:

I write in response to your letter of 27 August 2013 requesting information about intentional and willful misuse of surveillance authorities.

Since 1 January 2003, there have been 12 substantiated instances of intentional misuse of the signals intelligence (SIGINT) authorities of the Director of the National Security Agency. The NSA Office of the Inspector General (OIG) currently has two open investigations into alleged misuse of SIGINT and is reviewing one allegation for possible investigation.

1. Civilian Employee, Foreign Location

In 2011, before an upcoming reinvestigation polygraph, the subject reported that in 2004, "out of curiosity," he performed a SIGINT query of his home telephone number and the telephone number of his girlfriend, a foreign national. The SIGINT system prevented the query on the home number because it was made on a US person. The subject viewed the metadata returned by the query on his girlfriend's telephone.

The appropriate OIG conducted an investigation. The subject's actions were found to be in violation of United States Signals Intelligence Directive (USSID) 18 (Legal Compliance and U.S. Person Minimization Procedures).

The matter was referred to DoJ in 2011 for possible violations of 18 U.S.C. §641 (embezzlement and theft) and 18 U.S.C. §2511 (interception and disclosure of electronic communications). In 2011, DoJ declined prosecution. The subject retired in 2012 before disciplinary action had been taken.

2. Civilian Employee, Foreign Location

In 2005, during a pre-retirement reinvestigation polygraph and interview, the subject reported that, in 2003, he tasked SIGINT collection of the telephone number of his foreign-national girlfriend without an authorized purpose for approximately one month to determine whether she was "involved with any [local] government officials or other activities that might get [him] in trouble."

The NSA OIG determined that the subject's actions violated Executive Order 12333, DoD Regulation 5240.1-R, 5 C.F.R. § 2635.704, and NSA/CSS PMM 30-2, Chapter 366, §§ 1-3 and 3-1.

The OIG's report was shared with the NSA Office of General Counsel (OGC) for an assessment as to whether referral to DoJ was appropriate. Records are insufficient to determine whether a referral was made. The subject retired before the OIG investigation was finalized.

3. Civilian Employee, Foreign Location

In 2004, upon her return from a foreign site, the subject reported to NSA Security that, in 2004, she tasked a foreign telephone number she had discovered in her husband's cellular telephone because she suspected that her husband had been unfaithful. The tasking resulted in voice collection of her husband.

The NSA OIG determined that the subject's actions violated USSID 18, Executive Order 12333, 5 C.F.R. §2635.704, and DoD Regulation 5240.1-R, and possibly 18 U.S.C. §2511 (interception and disclosure of electronic communications).

The OIG report was forwarded to NSA's OGC, which referred the matter to DoJ. The subject of the investigation resigned before the proposed discipline of removal was administered

4. Civilian Employee, Foreign Location

In 2003, the appropriate OIG was notified that an employee had possibly violated USSID 18. A female foreign national employed by the U.S. government, with whom the subject was having sexual relations, told another government employee that she suspected that the subject was listening to her telephone calls. The other employee reported the incident.

The investigation determined that, from approximately 1998 to 2003, the employee tasked nine telephone numbers of female foreign nationals, without a valid foreign intelligence purpose, and listened to collected phone conversations while assigned to foreign locations. The subject conducted call chaining on one of the numbers and tasked the resultant numbers. He also incidentally collected the communications of a U.S. person on two occasions.

The appropriate agency referred the matter to DoJ. The subject was suspended without pay pending the outcome of the investigation and resigned before discipline had been proposed.

5. Civilian Employee, Foreign Location

The employee's agency discovered that an employee had misused the SIGINT collection system between 2001 and 2003 by targeting three female foreign nationals.

The appropriate OIG conducted an investigation. The violations were referred to DoJ. The subject resigned before disciplinary action was taken.

6. Civilian Employee, Foreign Location

As the result of a polygraph examination, it was discovered that an employee had accessed the collection of communications on two foreign nationals.

The employee's agency concluded its investigation in 2006, and the subject received a one-year letter of reprimand (prohibiting promotions, awards, and within-grade increases) and a 10 day suspension without pay. The subject's pending permanent-change-of-station assignment was cancelled, and his promotion recommendation was withdrawn.

7. Civilian Employee, Foreign Location

In 2011, the NSA OIG was notified that, in 2011, the subject had tasked the telephone number of her foreign-national boyfriend and other foreign nationals and that she reviewed the resultant collection. The subject reported this activity during an investigation into another matter.

The subject asserted that it was her practice to enter foreign national phone numbers she obtained in social settings into the SIGINT system to ensure that she was not talking to "shady characters" and to help mission.

The appropriate OIG found that the subject's actions potentially violated Executive Order 12333, Part 1.7(c)(1), and DoD Regulation 5240.1-R, Procedure 14.

The appropriate OIG referred the matter to DoJ in 2011 as a possible violation of 18 U.S.C. §2511 (interception and disclosure of electronic communications). The subject resigned before disciplinary action had been imposed.

8. Military Member, CONUS Site

In 2005, the NSA OIG was notified that, on the subject's first day of access to the SIGINT collection system, he queried six e-mail addresses belonging to a former girlfriend, a U.S. person, without authorization. A site review of SIGINT audit discovered the queries four days after they had occurred.

The subject testified that he wanted to practice on the system and had decided to use this former girlfriend's e-mail addresses. He also testified that he received no information as a result of his queries and had not read any U.S. person's e-mail.

The NSA OIG concluded that the subject's actions violated USSID 18, Executive Order 12333, 5 CFR §2635.704, and DoD Regulation 5240.1-R.

The OIG report was forwarded to the site command and the OGC. As a result of a Uniform Code of Military Justice Article 15 proceeding, the subject received a reduction in grade, 45 days restriction, 45 days of extra duty, and half pay for two months. It was recommended that the subject not be given a security clearance.

9. Civilian Employee, CONUS Site

In 2006, the Office of Oversight and Compliance within NSA's Signals Intelligence Directorate informed NSA OIG that, between 2005 and 2006, the subject had without authorization queried in two SIGINT systems the telephone numbers of two foreign nationals, one of whom was his girlfriend. On one occasion, the subject performed a text query of his own name in a SIGINT system.

The OIG investigation found that the subject queried his girlfriend's telephone number on many occasions and her name on two. He testified that he received only one "hit" from the queries on the girlfriend. Another number he queried, that of a foreign national language instructor, returned "insignificant information."

The subject claimed that he queried his name to see if anyone was discussing his travel and the telephone numbers to ensure that there were no security problems.

The OIG concluded that the subject's actions violated Executive Order 12333, 5 C.F.R. §2635.704, DoD Regulation 5240.1-R, and NSA/CSS PMM, Chapter 366 (General Principles for on the job conduct; Use of Government Resources, and Insubordination).

The Agency has been unable to locate records as to whether a referral was made to DoJ. The subject resigned from the Agency before the proposed discipline of removal had been administered.

10. Civilian Employee, CONUS Site

In 2008, the NSA OIG was notified that a SIGINT audit had discovered a possible violation of USSID 18. An investigation revealed that, while reviewing the communications of a valid intelligence target, the subject determined that the intelligence target had a relative in the U.S. The subject queried the SIGINT system for the e-mail address of the intelligence target in 2008 and used other search terms to obtain information about the target's relative.

The OIG concluded that the subject's actions violated USSID 18, Executive Order 12333, and DoD Regulation 5240.1-R.

The OIG report was forwarded to NSA's OGC. The subject received a written reprimand.

11. Military Member, Foreign Location

In 2009, the NSA OIG was notified that, in 2009, a military member assigned to a military tactical intelligence unit queried the communications of his wife, who was also a military member stationed in a foreign location. The misuse was discovered by a review of SIGINT audit logs. The investigation by his military unit substantiated the misuse.

Through a Uniform Code of Military Justice Article 15 proceeding, the member received a reduction in rank, 45 days extra duty, and half pay for two months. The member's access to classified information was revoked.

In 2009 this matter was referred to DoJ.

12. Military Member, Foreign Location

In 2009, a military unit at a foreign location notified the NSA OIG that, in 2009, a military member had queried a country's telephone numbers to aid in learning that country's language. The misuse was discovered by a review of SIGINT audit logs.

The appropriate branch of the military determined that the analyst's queries were not in support of his official duties and violated USSID 18.

The member's database access and access to classified information were suspended.

I hope that this information satisfies your request.

Sincerely,

George Ellard

Dr. George Ellard
Inspector General

cc: Sen. Patrick Leahy