United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510–6275

July 15, 2015

VIA ELECTRONIC TRANSMISSION

The Honorable James B. Comey, Jr.
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20535

The Honorable Chuck Rosenberg
Acting Administrator
Drug Enforcement Administration
700 Army Navy Drive, Room 12060
Arlington, VA 22202

The Honorable Michael J. Stella
Deputy Assistant Secretary of Defense
Department of Defense
1000 Defense Pentagon
Washington, DC 20301

Dear Director Comey, Acting Administrator Rosenberg, and Deputy Assistant Secretary Stella:

I am writing to inquire whether Hacking Team's representations in its spyware contracts with FBI, DEA, and DoD violated the Sudan Accountability and Divestment Act of 2007. On April 27, 2015, and June 12, 2015, I wrote to Deputy Attorney General Yates and Director Comey, respectively, to inquire about the use of spyware by the DEA and the FBI. Among other things, I wanted to know whether DEA or FBI had conducted business with Hacking Team, an Italian information technology and cybersecurity company. On July 8, 2015, I also chaired a hearing before the Senate Judiciary Committee entitled "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy." At that hearing, Deputy Attorney General Yates and Director Comey testified about the challenges that law enforcement is facing as a result of the widespread use of strong encryption and its ability to frustrate court-authorized wiretaps and search warrants. Some observers, including one of the hearing witnesses, have cited the lawful, court-authorized use of spyware by law enforcement as a potential way to address this problem.

Yesterday, I received a response to my April 27 letter from Assistant Attorney General Kadzik, which provided substantive answers to my questions regarding the DEA's use of spyware. That letter confirmed that DEA had a business relationship with Hacking Team beginning in 2012, and explained how DEA acted pursuant to relevant legal authorities and agency procedures in its use of the company's spyware. It also revealed that, although its contract with Hacking Team extends to the end of 2015, the DEA recently terminated the contract.

Between the transmittal of my letters and my receipt of the DEA's response, Hacking Team was itself hacked, and a number of the company's internal emails and documents were leaked to the public. Subsequent reporting on the documents detailed Hacking Team's business relationships with the DEA, the FBI, and the DoD.[1] In addition to Hacking Team's relationships with legitimate law enforcement and military buyers, it is troubling that the leaked documents also revealed Hacking Team's business relationships with a number of repressive regimes around the world, including Sudan.[2] While it is vital that U.S. law enforcement and our military have the technological tools needed to investigate terrorists and criminals in order to keep the public safe, it is also important that we acquire those tools from responsible, ethical sources who are acting in accordance with the law.

As you know, the Sudan Accountability and Divestment Act of 2007 ("the Act'), PL 110-174, and its implementing regulation, 48 CFR 25.702, prohibit the United States Government from entering into contracts with any contractor conducting certain types of restricted business with Sudan, including the sale of "military equipment," which the Act defines as:

> (A) weapons, arms, military supplies, and equipment that readily may be used for military purposes,[. . .]; or

---

[1] *E.g.*, Lorenzo Franceschi-Bicchierai, *Spy Tech Company "Hacking Team" Gets Hacked*, MOTHERBOARD, July 5, 2015; Cory Bennett, *Hack at Surveillance Firm Exposes Ties to FBI, DEA*, THE HILL, July 6, 2015; Cora Currier and Morgan Marquis-Boire, *Leaked Documents Show FBI, DEA, and U.S. Army Buying Italian Spyware*, THE INTERCEPT, July 6, 2015; Joseph Cox, *The FBI Spent $775k on Hacking Team's Spy Tools Since 2011*, WIRED, July 6, 2015; Jennifer Valentino-Devries and Danny Yadron, *Hacking Team, the Surveillance Tech Firm, Gets Hacked*, THE WALL STREET JOURNAL, July 6, 2015.

[2] Dell Cameron, *Hacking Team Sold Spy Tools to Oppressive Sudanese Government*, THE DAILY DOT, July 6, 2015; Lauren Walker, *Cybersecurity Company Supplies Repressive Regimes with Spyware, Recent Hack Claims*, NEWSWEEK, July 6, 2015; Shane Harris, *U.S. Hired Dictators' Favorite Hackers*, THE DAILY BEAST, July 6, 2015; Tim Cushing, *Hacking Team Hacked: Documents Show Company Sold Exploits and Spyware to UN-Blacklisted Governments*, TECHDIRT, July 6, 2015; Cora Currier and Morgan Marquis-Boire, *A Detailed Look at Hacking Team's Emails About Its Repressive Clients*, THE INTERCEPT, July 7, 2015; Jose Pagliery, *This Company Sells Spy Tools to Evil Governments*, CNN MONEY, July 6, 2015; Samuel Gibbs, *Hacking Team Boss: We Sold to Ethiopia But 'We're the Good Guys,'* THE GUARDIAN, July 13, 2015 (in an interview, Hacking Team founder "admitted providing tools to […] Sudan").

(B) supplies or services sold or provided directly or indirectly to any force actively participating in armed conflict in Sudan.

PL 110-174.[3] In order to prevent the government from entering into such prohibited contracts, the Act requires the head of each executive agency to ensure that each contract entered into by the agency for the procurement of goods or services includes a clause that requires the contractor to certify that it does not conduct restricted business operations in Sudan. The Act further provides that if the head of a government agency determines that the contractor has submitted a false certification, he or she may impose remedies, including terminating the contract and debarring or suspending the contractor from eligibility for Federal contracts. Under the Act, the General Services Administrator is to include on the GSA's List of Parties Excluded from Federal Procurement each contractor that is debarred, suspended, proposed for debarment or suspension, or declared ineligible by the head of an executive agency on the basis of a determination of a false certification.

Assistant Attorney General Kadzik's letter stated the DEA's business relationship with Hacking Team began in 2012. According to press reports, Hacking Team's business relationships with FBI and the Army began in 2011.[4] Hacking Team's internal documents reveal that in 2012 the company sold its spyware to Sudan's National Intelligence and Security Service for 960,000 euros, and that this relationship continued until late 2014.[5] In June of 2014, the United Nations panel monitoring the implementation of sanctions against Sudan began investigating Hacking Team's alleged contract with Sudan, writing to the company to seek information.[6] Hacking Team did not immediately respond. Months later, in November of 2014, internal Hacking Team documents stated that its business with Sudan was "unofficially suspended, on-hold."[7] In January of 2015, Hacking Team finally responded to the U.N.,

---

[3] Some spyware and other types of malware readily may be used for military purposes. *See* Department of Defense, LAW OF WAR MANUAL, *Chapter XVI: Cyber Operations* 994-1008, June, 2015. As explained in the Senate Report on the Sudan Accountability and Divestment Act of 2007, the Act's definition of restricted "military equipment" is meant to include "dual use" items unless "it can be credibility proven that these items will not be used for any military purpose." S. Rep. 110-213. Moreover, Hacking Team reportedly sold its spyware to Sudan's National Intelligence Security Service. *Infra* n. 5. "[T]he head of National Intelligence Security Services [. . . was] among the key figures ordering and coordinating the violence in Darfur." Emily Wax, *U.S. Report Finds Sudan Promoted Killings; Use of Term 'Genocide' Debated Ahead of Powell Testimony on Darfur Atrocities*, THE WASHINGTON POST, Sep. 8, 2004.

[4] *Supra* n. 1.

[5] Cora Currier and Morgan Marquis-Boire, *A Detailed Look at Hacking Team's Emails About Its Repressive Clients*, THE INTERCEPT, July 7, 2015.

[6] *Id*.; *see* Tim Cushing, *Hacking Team Hacked: Documents Show Company Sold Exploits and Spyware to UN-Blacklisted Governments*, TECHDIRT, July 6, 2015. Hacking Team's suspected business with Sudan was first publicly noted in a 2014 report by Citizen Lab, which is based at the University of Toronto and researches the intersection of information technology and human rights. *See* Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, *Mapping Hacking Team's "Untraceable" Spyware*, THE CITIZEN LAB, Feb. 17, 2014.

[7] *Supra* n. 5.

claiming –in the present tense– that the company has no "current sales relationship" with Sudan.[8] In a subsequent letter, Hacking Team reportedly argued that its spyware does not qualify as weaponized software that would run afoul of U.N. sanctions against Sudan. The U.N. disagreed, writing:

> The view of the panel is that as such software is ideally suited to support military electronic intelligence (ELINT) operations it may potentially fall under the category of 'military … equipment' or 'assistance' related to prohibited items. Thus its potential use in targeting any of the belligerents in the Darfur conflict is of interest to the Panel.[9]

The recent leak of Hacking Team's internal documents seems to vindicate the U.N.'s suspicions, and this week Hacking Team's founder reportedly admitted the company's business with Sudan.[10] Since the leak, at least one European official has also asked Italy and the European Commission to investigate whether Hacking Team's sales to Sudan and Russia violated European sanctions against those countries.[11]

In light of DEA's acknowledgement of its business with Hacking Team, the reports of Hacking Team's business with FBI and DoD, and Hacking Team's concomitant business with Sudan, the question arises as to whether the contracts the company had with U.S. agencies were in violation of the Sudan Accountability and Divestment Act of 2007. In order for the Committee to evaluate whether this was the case, please respond to the following by no later than July 29, 2015:

1. Please describe in detail any contract, agreement, training, or other business the FBI and DoD has ever had with Hacking Team, its resellers, or its affiliated companies.[12] Does the FBI or DoD currently have a business relationship with Hacking Team, its resellers, or its affiliated companies?

2. In keeping with the requirements of the Sudan Accountability and Divestment Act of 2007, did the DEA, FBI, and DoD contracts for procurement of goods or services from Hacking Team, its resellers, or its affiliated companies include a

---

[8] *Id.*; Cushing *supra* n. 6.
[9] *Id.*
[10] Gibbs *supra* n. 2 (in an interview, Hacking Team founder "admitted providing tools to […] Sudan").
[11] Lorenzo Franceshi-Bicchierai, *Italy Should Investigate Hacking Team, European Parliament Member Says*, MOTHERBOARD, July 7, 2015.
[12] According to press reports, Hacking Team has used a variety of partner companies in selling its spyware. *See* Joshua Kopstein, *Meet the Companies that Helped Hacking Team Sell Tools to Repressive Governments*, MOTHERBOARD, July 9, 2015; Lorenzo Franceschi-Bicchierai, *The DEA Has Been Secretly Buying Hacking Tools From an Italian Company*, MOTHERBOARD, April 15, 2015.

clause requiring the contractor to certify that it does not conduct restricted business operations in Sudan? If so, please provide copies of all such contracts, including any contracts for licenses, training, upgrades, technical support, and renewal of services. If not, why not?

3. If such certifications were included in the contracts, in light of the reports of Hacking Team's business relationship with Sudan, has FBI, DEA, or DoD evaluated whether Hacking Team, its resellers, or its affiliated companies submitted a false certification? If so, please provide copies of all documents relating to such evaluations. If not, why not?

4. If FBI, DEA, or DoD has determined that the contracts with Hacking Team, its resellers, or its affiliated companies contained false certifications, have you taken any of the remedial actions provided in the Act, including terminating the contract and debarring or suspending Hacking Team from eligibility for future Federal contracts? Have you reported such determination to the Administrator of General Services so she may include Hacking Team on the List of Parties Excluded from Federal Procurement? If so, please provide copies of all documents relating to such remedial actions. If not, why not? Did DEA terminate its contract with Hacking Team on the basis of a false certification?

5. If you have determined that the contracts with Hacking Team, its resellers, or its affiliated companies contained false certifications with regard to Sudan, have you referred the matter to the appropriate sections of the Department of Justice to investigate whether such false certifications or the underlying business with Sudan constituted a criminal matter? If so, please provide copies of such referrals. If not, why not?

Please number your answers according to their corresponding questions. If you have any questions about this request, feel free to contact Patrick Davis of my Committee staff at (202) 224-5225. Thank you for your attention to this important matter.

Charles E. Grassley

Chairman
Senate Committee on the Judiciary