

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

**Holding a Criminal Term
Grand Jury Sworn in on May 7, 2019**

UNITED STATES OF AMERICA	:	CRIMINAL NO.
	:	
v.	:	GRAND JURY ORIGINAL
	:	
CHARLES KUMAR EDWARDS and MURALI YAMAZULA VENKATA,	:	VIOLATIONS:
	:	
Defendants.	:	18 U.S.C. § 371 (Conspiracy to Commit Theft of Government Property and to Defraud the United States)
	:	18 U.S.C. § 641 (Theft of Government Property)
	:	18 U.S.C. § 1343 (Wire Fraud)
	:	18 U.S.C. § 1028A (Aggravated Identity Theft)
	:	18 U.S.C. § 1519 (Destruction of Records)
	:	18 U.S.C. § 2 (Aiding and Abetting; Causing an Act to be Done)

INDICTMENT

The Grand Jury charges that:

Introduction

At all times material to this Indictment:

1. The core mission of the U.S. Department of Homeland Security – Office of Inspector General (“DHS-OIG”) is to provide independent oversight and to promote excellence, integrity, and accountability within the U.S. Department of Homeland Security (“DHS”). DHS-OIG Headquarters was located at 1120 Vermont Avenue, N.W., Washington, D.C.

2. Defendant CHARLES KUMAR EDWARDS worked for DHS-OIG from in and around February 2008 to in and around December 2013, including as DHS-OIG’s Acting Inspector General. Prior to working at DHS-OIG, Defendant EDWARDS worked at the Transportation

Security Administration (“TSA”) and the U.S. Postal Service – Office of Inspector General (“USPS-OIG”). After leaving DHS-OIG, Defendant EDWARDS founded Delta Business Solutions, Inc. (“DBS”), a Maryland corporation, in and around September 2015.

3. Defendant MURALI YAMAZULA VENKATA worked as an Information Technology (“IT”) Specialist in the IT Division at DHS-OIG Headquarters. When VENKATA joined DHS-OIG in and around June 2010, he signed a Computer Access Agreement in which he acknowledged:

I will protect displayed, stored data, magnetic media, printouts in accordance with the highest level of data sensitivity contained on that media. I will follow OIG policy for transmitting sensitive data (such as name, ssn, home address, etc.) by utilizing WinZip or other OIG standard encryption software.

In his signed Computer Access Agreement, Defendant VENKATA further acknowledged:

I will not remove DHS computer systems or software from Government work spaces without express written permission. I understand I am personally responsible for providing physical security and keeping items under my exclusive control.

Prior to joining DHS-OIG in and around June 2010, Defendant VENKATA worked at USPS-OIG. While at DHS-OIG, Defendant VENKATA did not request or receive any authorizations for outside employment.

4. Sonal Patel worked as an Enterprise Applications Branch Chief in the IT Division at DHS-OIG Headquarters. Patel oversaw the development and maintenance of DHS-OIG’s Enforcement Database System (“EDS”). When Patel joined DHS-OIG in February 2009, she signed a Computer Access Agreement in which she acknowledged:

I will protect displayed, stored data, magnetic media, printouts in accordance with the highest level of data sensitivity contained on that media. I will follow OIG policy for transmitting sensitive data (such as name, ssn, home address, etc.) by utilizing WinZip or other OIG standard encryption software.

In her signed Computer Access Agreement, Patel further acknowledged:

I will not remove DHS computer systems or software from Government work spaces without express written permission. I understand I am personally responsible for providing physical security and keeping items under my exclusive control.

Prior to joining DHS-OIG in and around February 2009, Patel worked at TSA and USPS-OIG. While at DHS-OIG, Patel did not request or receive any authorizations for outside employment.

5. While at DHS-OIG, Defendant EDWARDS supervised Patel, both directly and indirectly. Defendant EDWARDS began supervising Patel at USPS-OIG when Defendant EDWARDS was the Director of Information Technology and the Deputy Chief Information Officer. At DHS-OIG, Patel supervised Defendant VENKATA. While at USPS-OIG, Patel worked on USPS-OIG's case management systems, including USPS-OIG's STARS database, which was used primarily for investigations and audits, as well as USPS-OIG's Performance and Results Information System ("PARIS"), which USPS-OIG employees used to interface with the STARS database. In and around 2009, Defendant EDWARDS provided Patel with a CD containing USPS-OIG's STARS database, source code, scripts, and file server contents, which included the personally identifiable information ("PII") of USPS employees. Defendant EDWARDS had Patel copy the contents of the CD onto the DHS-OIG server to enhance DHS-OIG's audit systems.

6. DBS was founded by Defendant EDWARDS on or about September 2, 2015, as a Maryland Stock Corporation. The principal office address for DBS was located at Defendant EDWARDS's residence in Sandy Spring, Maryland.

7. Company A was a software development company based in Bangalore, India.

8. EDS was the case management system used by the DHS-OIG Office of Investigations. In and around 2008, DHS obtained ownership rights to the EDS source code. Since in and around 2008, DHS-OIG has substantially modified and enhanced the EDS system. The

initial contract for the EDS system cost DHS approximately \$3,161,620.30. One substantial modification to EDS was the creation of an “eSubpoena” module. The functional specifications for the module were finalized on or about September 29, 2014. Patel oversaw the development and implementation of this module by government employees and government contractors working under her. These employees included Defendant VENKATA, who was the principal developer of this module.

9. DHS-OIG also owned and maintained Multiple Activation Keys and a Key Management Services Code associated with various Microsoft software products. These Multiple Activation Keys and Key Management Services Code, which could be used to download Microsoft software products without payment, were the property of DHS-OIG and the United States Government and had a value of approximately \$348,362.00.

COUNT ONE

(Conspiracy to Commit Theft of Government Property and to Defraud the United States)

10. The allegations set forth in paragraphs 1 through 9 of this Indictment are realleged and incorporated by reference.

11. From in and around October 2014 to in and around April 2017, within the District of Columbia and elsewhere, Defendants EDWARDS and VENKATA, and Patel, did knowingly and willfully conspire, combine, confederate, and agree together and with each other, and with others known and unknown to the Grand Jury:

a. to commit offenses against the United States, that is: to willfully and knowingly steal, purloin, and convert copies of DHS-OIG’s EDS system, copies of DHS-OIG’s EDS source code and database files, copies of USPS-OIG’s case management system, copies of USPS-OIG’s STARS database and PARIS system, the PII of approximately 246,167 DHS employees and approximately 6,723 U.S. Postal Service (“USPS”) employees, and Multiple

Activation Keys and a Key Management Services Code associated with various Microsoft software products, of a value exceeding \$1,000, of goods and property of the United States, in violation of 18 U.S.C. § 641; and

b. to defraud the United States by devising and intending to devise a scheme to defraud and for obtaining money and property from the U.S. Department of Agriculture – Office of Inspector General (“USDA-OIG”) means of materially false and fraudulent pretenses, representations, and promises, and by concealing material facts.

The Purposes of the Conspiracy

12. It was a purpose of the conspiracy for Defendants EDWARDS and VENKATA and Patel to use their positions to access, copy, steal, purloin, and convert (1) DHS-OIG’s EDS system; (2) DHS-OIG’s EDS source code, including the eSubpoena module; (3) DHS-OIG’s database, which included the PII of DHS employees; and (4) USPS-OIG’s STARS database and PARIS system, which included the PII of USPS employees; so that Defendant EDWARDS and his business DBS could create and develop a private, commercially owned version of a case management system to be offered for sale to government agencies for the benefit, enrichment, and profit of Defendant EDWARDS and his business DBS.

13. It also was a purpose of the conspiracy for Defendant VENKATA and Patel to use their positions at DHS-OIG to access and copy Multiple Activation Keys and a Key Management Services Code associated with various Microsoft software products for Defendant EDWARDS and his business DBS to assist with the creation and development of a private, commercially owned version of a case management system to be offered for sale to government agencies for the benefit, enrichment, and profit of Defendant EDWARDS and his business DBS.

14. It also was a purpose of the conspiracy for Defendants EDWARDS and VENKATA

and Patel to conceal from DHS-OIG, USDA-OIG, and others the theft and provision of (1) DHS-OIG's EDS system; (2) DHS-OIG's EDS source code, including the eSubpoena module; and (3) DHS-OIG's database, which included the PII of DHS employees, to Defendant EDWARDS.

Manner and Means of the Conspiracy

15. The manner and means by which these purposes were carried out included the following:

a. Defendant VENKATA and Patel accessed and copied (1) DHS-OIG's EDS system; (2) DHS-OIG's EDS source code, including the eSubpoena module; (3) DHS-OIG's database, which included the PII of DHS employees; and (4) USPS-OIG's STARS database and PARIS system, which included the PII of USPS employees, which Defendant VENKATA and Patel delivered and transmitted to Defendant EDWARDS after Defendant EDWARDS had left his employment with DHS-OIG.

b. Defendant VENKATA and Patel accessed and copied Multiple Activation Keys and a Key Management Services Code associated with various Microsoft software products, which Defendant VENKATA and Patel delivered and transmitted to Defendant EDWARDS.

c. Defendant VENKATA and Patel transmitted DHS-OIG and USPS-OIG documents and information to Defendant EDWARDS to assist Defendant EDWARDS with the creation and development of a private, commercially owned version of a case management system to be offered for sale to government agencies for the benefit, enrichment, and profit of Defendant EDWARDS and his business DBS.

d. Defendant VENKATA and Patel accessed Defendant EDWARDS's laptop and computer servers containing the case management system under development to provide technical and configuration advice, assistance, and support to Defendant EDWARDS and his

business DBS.

e. Defendant EDWARDS used, possessed, and transferred stolen DHS-OIG and USPS-OIG documents and information, including PII of DHS and USPS employees, to software developers in India who were assisting Defendant EDWARDS with the creation and development of a private, commercially owned version of a case management system to be offered for sale to government agencies for the benefit, enrichment, and profit of Defendant EDWARDS and his business DBS.

f. Defendants EDWARDS and VENKATA and Patel concealed their theft and the provision of software, source code, databases, documents, information, and PII to Defendant EDWARDS by arranging roadside meetings to pass media and equipment to Defendant EDWARDS, by emailing documents to their personal email accounts before forwarding them on to Defendant EDWARDS, and by concealing from DHS-OIG employees the purpose of their request for software.

g. Defendant EDWARDS and Patel concealed their theft of EDS-related software, source code, databases, documents, information, and PII from USDA-OIG through false and fraudulent pretenses, representations, and promises to Witness One to encourage and induce USDA-OIG into purchasing EDS 2.0 for the benefit, enrichment, and profit of Defendant EDWARDS and his business DBS.

Overt Acts

16. In furtherance of the conspiracy, and in order to effect the objects thereof, Defendants EDWARDS and VENKATA, Patel, and co-conspirators not indicted herein who are both known and unknown to the Grand Jury, in various combinations, directly and indirectly, within the District of Columbia and elsewhere, committed overt acts, including, but not limited to,

the following:

a. On or about October 14, 2014, after Defendant EDWARDS had left DHS-OIG, Patel copied the EDS source code, which included the eSubpoena module, and database files from the DHS-OIG computer network onto an optical disk.

b. On or about November 4, 2014, Patel instructed a subordinate DHS-OIG employee to send Patel instructions on how to install the EDS system. Patel concealed the purpose for which she was requesting the instructions. Patel caused the DHS-OIG employee to provide Patel with instructions on how to rebuild the EDS system on an alternate server.

c. On or about November 4, 2015, Patel sent, from her personal Yahoo! email account to Defendant EDWARDS's personal Verizon email account, a list of Multiple Activation Keys and a Key Management Services Code associated with various Microsoft software products licensed to DHS-OIG.

d. On or about December 1, 2015, Patel called an employee at USDA-OIG ("Witness One") to discourage USDA-OIG from acquiring EDS from DHS-OIG free of charge based on a Memorandum of Understanding between the agencies. Patel told Witness One that she thought USDA-OIG would be better served by EDS 2.0, a commercial product being developed by Defendant EDWARDS, with Patel's and Defendant VENKATA's assistance. Patel further stated that she and Defendant EDWARDS would like to meet with Witness One to discuss EDS 2.0.

e. On or about May 6, 2016, Patel promoted EDS 2.0 to Witness One by describing EDS 2.0 as having the same modules and feel as EDS, but with a more modular, plug-and-play design.

f. On or about May 10, 2016, Patel emailed, from her DHS-OIG government

email account, Witness One asking to meet Witness One for lunch to discuss EDS 2.0.

g. On or about May 12, 2016, Defendant VENKATA and Patel exchanged text messages to coordinate a meeting with Defendant EDWARDS to discuss EDS 2.0.

h. On or about May 25, 2016, Patel emailed, from her DHS-OIG government email account, Witness One to confirm a lunch meeting with Defendant EDWARDS to discuss EDS 2.0.

i. On or about May 25, 2016, Patel sent, from her personal Yahoo! email account to Defendant EDWARDS's personal Verizon email account, a list of the key benefits of EDS 2.0.

j. On or about May 26, 2016, Patel and Defendant EDWARDS met with Witness One at a restaurant in the District of Columbia. At that meeting, Patel and Defendant EDWARDS discussed the benefits of EDS 2.0 and the disadvantages of DHS-OIG's EDS. During the meeting, Patel stated that she could "tell him [Defendant EDWARDS] the concepts" of eSubpoena so that Defendant EDWARDS could incorporate eSubpoena into EDS 2.0. Patel further stated that Defendant VENKATA could incorporate eSubpoena into EDS 2.0. Defendant EDWARDS stated that he would give Patel his input so that the costs for USDA-OIG to purchase EDS 2.0 could be developed. Defendant EDWARDS and Patel also discussed providing the original version of EDS to Witness One on a laptop for Witness One to show his supervisors in the short term that he was not "dragging [his] feet" on obtaining a case management system while Defendant EDWARDS and Patel developed EDS 2.0. Defendant EDWARDS and Patel informed Witness One that he would just need to provide specifications to ensure that the laptop would be compatible with USDA-OIG's systems. Patel indicated that she would send the specifications to Witness One. At no point did Patel or EDWARDS disclose that EDS 2.0 had been built based on

the original EDS software that they had stolen from DHS-OIG and USPS-OIG.

k. On or about May 27, 2016, Patel copied DHS-OIG's EDS source code and database from the DHS-OIG computer network onto optical disks in order to provide them to Defendant EDWARDS to aid in his development of EDS 2.0. On or about May 27, 2016, Patel also sent, from her DHS-OIG government email account to her personal Yahoo! email account, a government document containing detailed instructions for rebuilding DHS-OIG's EDS web applications from backup files onto another server. Also on or about May 27, 2016, Patel forwarded that document from her personal Yahoo! email account to Defendant EDWARDS's personal Verizon email account.

l. On or about May 28, 2016, Defendant VENKATA and Patel exchanged text messages about meeting with Defendant EDWARDS at Patel's home on May 30, 2016 (Memorial Day).

m. On or about May 30, 2016, Patel and Defendants EDWARDS and VENKATA met at Patel's residence in Sterling, Virginia. During the meeting, Patel and Defendant VENKATA showed Defendant EDWARDS improvements that had been made to DHS-OIG's EDS system since Edwards's departure from DHS-OIG, including the addition of the eSubpoena module. Patel and Defendants EDWARDS and VENKATA discussed technology for EDS 2.0 based on USPS-OIG's case management system and DHS-OIG's EDS.

n. On or about May 31, 2016, Patel sent an email, from her DHS-OIG government email account, to Witness One providing the software specifications required for the laptop to ensure that Witness One would be able to access the original version of EDS.

o. In and around June 2016, Defendant EDWARDS hired a software development company in India to assist in the development of EDS 2.0. Defendant EDWARDS

told these programmers that he would provide them with the eSubpoena requirements, a complete working version of the system, and the code, with the assistance of Patel.

p. On or about June 27, 2016, Defendant VENKATA sent, from his DHS-OIG government email account to Patel's DHS-OIG government email account, technical instructions relating to DHS-OIG's EDS system. Patel first sent these instructions from her DHS-OIG government email account to her personal Yahoo! email account and then forwarded those instructions from her Yahoo! email account to Defendant EDWARDS's personal Verizon email account.

q. On or about June 30, 2016, Patel and Defendant EDWARDS participated in an online meeting with the Indian software development company. Defendant EDWARDS provided the software developers with remote access over the Internet to the EDS source code and DHS-OIG database files that Patel had provided to Defendant EDWARDS and that Defendant EDWARDS had saved on a non-government server in his residence.

r. On or about July 8, 2016, Defendant EDWARDS sent a text message to Witness One informing him that EDS 2.0 would be ready in mid- to late-September.

s. On or about July 8, 2016, Defendant VENKATA sent, from his DHS-OIG government email account to Patel's DHS-OIG government email account, a government document containing the functional requirements for the eSubpoena module. Also on or about July 8, 2016, and then again on or about July 20, 2016, Patel sent that document from her DHS-OIG government email account to her personal Yahoo! email account. On or about July 8, 2016, Patel forwarded that email and document from her personal Yahoo! email account to Defendant EDWARDS's personal Verizon email account.

t. On or about July 9, 2016, Defendant EDWARDS and Company A signed

an agreement for Company A to assist Defendant EDWARDS and DBS in the development of an Investigations Management System for Offices of Inspectors General.

u. On or about July 13, 2016, Defendant VENKATA and Patel exchanged text messages about copying files and source code for Defendant EDWARDS onto a laptop provided by Defendant EDWARDS.

v. On or about July 13, 2016, Defendant EDWARDS delivered a laptop to Patel at DHS-OIG Headquarters and Patel delivered it to Defendant VENKATA. Patel requested that Defendant VENKATA check the laptop computer to determine whether fresh downloads of DHS-OIG's EDS source code and database files were needed, or whether the laptop computer just needed to be configured.

w. On or about July 13, 2016, Defendant EDWARDS sent an email to Witness One informing him that the "next gen" version of DHS-OIG's EDS would be ready around the middle of September.

x. On or about July 15, 2016, Defendant VENKATA returned the reconfigured laptop computer to Defendant EDWARDS by delivering it to him at a jewelry store in Tysons Corner, Virginia.

y. On or about July 20, 2016, Defendant EDWARDS provided Defendant VENKATA with access to the server in Defendant EDWARDS's residence for Defendant VENKATA to perform work on configuring and developing the case management system.

z. On or about August 1, 2016, Defendant EDWARDS wired \$204.00 to Company A for "Payment for Services."

aa. On or about August 3, 2016, Defendant EDWARDS wired \$10,955.00 to Company A.

bb. On or about August 6, 2016, Defendant EDWARDS traveled from Washington Dulles International Airport to Bangalore, India, to meet with software developers for the purpose of developing EDS 2.0. Because Defendant EDWARDS was having trouble getting the system to work on his home server, he asked for Patel to provide him with a copy of DHS-OIG's EDS source code and data. Patel met Defendant EDWARDS on the side of a road in Virginia as Defendant EDWARDS was on his way to Washington Dulles International Airport and provided to Defendant EDWARDS two DVDs containing DHS-OIG's EDS source code and data. Defendant EDWARDS also brought the reconfigured laptop computer, which Defendant VENKATA had delivered to him at a jewelry store on or about July 15, 2016, with him to India.

cc. On or about October 12, 2016, Defendant EDWARDS provided an update to Witness One indicating that his team had built the full version of the EDS system, which would be ready by mid-December, that he had addressed all of the concerns Witness One had raised in their meeting, and that the system had eSubpoena "just like DHS has." Defendant EDWARDS offered to meet Witness One to show him the "demo version" on a laptop or could allow Witness One to log into the live version, which was hosted on Defendant EDWARDS's server. Witness One requested a cost proposal from Defendant EDWARDS.

dd. On or about October 13, 2016, Defendant EDWARDS sent an email to Witness One with potential dates and times for the EDS 2.0 product demonstration.

ee. On or about October 23, 2016, Defendant EDWARDS sent several WhatsApp messages to the developers in India informing them that his "prospective contract" wanted to see the system under development in December but that he wanted to meet in November to discuss the system.

ff. On or about November 2, 2016, Patel sent, from her personal Yahoo! email

account to Defendant EDWARDS's Verizon email account, U.S. General Services Administration public information on pricing case management systems for Patel and Defendant EDWARDS to use as a basis for pricing EDS 2.0 for Witness One.

gg. On or about November 2, 2016, Defendant EDWARDS met with Witness One at USDA Headquarters in the District of Columbia. During the meeting, Defendant EDWARDS stated that EDS 2.0 contained an eSubpoena module, which he described as the same as the DHS-OIG version but faster and with a better flow. Defendant EDWARDS further informed Witness One that his team "went through and broke it apart, and each template we built back the way it was supposed to load."

hh. On or about November 8, 2016, Defendant EDWARDS participated in calls and online meetings with the developers in India.

ii. On or about December 21, 2016, Defendant EDWARDS wired \$5,000.00 to Company A for "Full Payment for Delta Business Website Development and Deployment."

jj. On or about January 3, 2017, Defendant EDWARDS left a voicemail for Witness One on his USDA-OIG office phone in the District of Columbia. In the voicemail, Defendant EDWARDS stated that Patel was working with him to develop EDS 2.0, and that he would have the system ready for Witness One in January to test.

kk. In and around March 2017, Defendants EDWARDS and VENKATA continued to work together on the system hosted on Defendant EDWARDS's server. Defendant VENKATA restored DHS-OIG's EDS databases on, and fixed the configuration within, the system. Defendant VENKATA also assisted Defendant EDWARDS install and configure PARIS, with data imported from STARS, on another server in his residence to assist the developers in India in seeing how the system under development should work.

ll. On or about March 15, 2017, Defendant EDWARDS provided Defendant VENKATA with remote login information for PARIS, which was hosted on Defendant EDWARDS's server.

mm. On or about March 21, 2017, Patel once again copied the USPS-OIG database, source code, scripts, and file server contents (which Patel had previously uploaded to DHS-OIG's server in and around 2009 at Defendant EDWARDS's instruction), from the DHS-OIG server onto two DVDs. Patel provided the two DVDs to Defendant VENKATA for delivery to Defendant EDWARDS. Defendant VENKATA met Defendant EDWARDS outside of DHS-OIG Headquarters in the District of Columbia, and delivered the DVDs to Defendant EDWARDS.

nn. On or about March 30, 2017, Defendant EDWARDS again traveled to India to meet with the Indian developers. While Defendant Edwards was in India, Defendant EDWARDS called Patel for her assistance in explaining the database to the developers.

**(Conspiracy Commit Theft of Government Property and to Defraud the United States,
in violation of Title 18, United States Code, Section 371)**

COUNT TWO
(Theft of Government Property)

17. The allegations set forth in paragraphs 1 through 16 of this Indictment are realleged and incorporated by reference.

18. From in and around October 2014 through in and around April 2017, within the District of Columbia and elsewhere, Defendants EDWARDS and VENKATA, did willfully and knowingly steal, purloin, and convert copies of DHS-OIG's EDS system, copies of DHS-OIG's EDS source code and database files, copies of USPS-OIG's case management system, copies of USPS-OIG's STARS database and PARIS system, the PII of approximately 246,167 DHS employees and approximately 6,723 USPS employees, and Multiple Activation Keys and a Key

Management Services Code associated with various Microsoft software products, of a value exceeding \$1,000, of goods and property of the United States.

**(Theft of Government Property
and Aiding and Abetting and Causing an Act to be Done,
in violation of Title 18, United States Code, Sections 641 and 2)**

**COUNTS THREE THROUGH ELEVEN
(Wire Fraud)**

19. The allegations set forth in paragraphs 1 through 16 of this Indictment are realleged and incorporated by reference.

20. From in and around October 2014 through in and around April 2017, within the District of Columbia and elsewhere, Defendants EDWARDS and VENKATA, knowingly devised a scheme to defraud USDA-OIG, and to obtain property of USDA-OIG by means of materially false and fraudulent pretenses, representations, and promises, and by concealing material facts.

21. On or about the dates set forth below, in the District of Columbia and elsewhere, Defendant EDWARDS, for the purpose of executing the aforementioned scheme and artifice, did transmit and cause to be transmitted by means of wire communication in interstate commerce the following writings, signs, signals, and sounds:

Count	Date	Wire Transmission
Three	May 25, 2016	Email from Patel's DHS-OIG government email account in the District of Columbia to Witness One's USDA-OIG government email account outside the District of Columbia confirming the Thursday, May 26, 2016, 12:30 p.m. lunch meeting between Defendant EDWARDS, Patel, and Witness One at a restaurant in the District of Columbia.
Four	May 27, 2016	Email from Patel's DHS-OIG government email account in the District of Columbia to her personal Yahoo! email account outside the District of Columbia attaching a government document containing detailed instructions for rebuilding the EDS web applications from backup files onto another server. Patel then forwarded that document from her personal Yahoo! email account to Defendant EDWARDS's personal Verizon email account.

Count	Date	Wire Transmission
Five	May 31, 2016	Email from Patel's DHS-OIG government email account in the District of Columbia to Witness One's USDA-OIG government email account outside the District of Columbia containing software specification requirements for laptop containing EDS development and code, as discussed during the Thursday, May 26, 2016, 12:30 p.m. lunch meeting between Defendant EDWARDS, Patel, and Witness One at a restaurant in the District of Columbia.
Six	June 27, 2016	Email from Patel's DHS-OIG government email account in the District of Columbia to her personal Yahoo! email account outside the District of Columbia forwarding technical instructions relating to the EDS system. Also on June 27, 2016, Patel forwarded those instructions from her Yahoo! email account to Defendant EDWARDS's Verizon email account.
Seven	July 8, 2016	Email from Patel's DHS-OIG government email account in the District of Columbia to her personal Yahoo! email account outside the District of Columbia attaching a government document containing the detailed functional requirements developed by DHS-OIG to design the eSubpoena module for EDS. Patel forwarded that document from her personal Yahoo! email account outside the District of Columbia to Defendant EDWARDS's personal Verizon email account.
Eight	November 2, 2016	Telephone call from Defendant EDWARDS's cell phone to Witness One's USDA-OIG office phone in the District of Columbia.
Nine	January 3, 2017	Telephone call from Defendant EDWARDS's cell phone to Witness One's USDA-OIG office phone in the District of Columbia leaving voicemail discussing EDS 2.0.
Ten	March 21, 2017	WhatsApp message from Defendant EDWARDS to Patel in which Defendant EDWARDS requested Patel to copy DVDs containing government software and information.

22. On or about the dates set forth below, in the District of Columbia and elsewhere, Defendants EDWARDS and VENKATA, for the purpose of executing the aforementioned scheme and artifice, did transmit and cause to be transmitted by means of wire communication in interstate commerce the following writings, signs, signals, and sounds:

Count	Date	Wire Transmission
Eleven	March 22, 2017	Telephone call from Defendant EDWARDS's cell phone to Defendant VENKATA's cell phone to arrange for Defendant

Count	Date	Wire Transmission
		EDWARDS to pick up DVDs containing government software and information in the District of Columbia.

**(Wire Fraud,
in violation of Title 18, United States Code, Section 1343)**

**COUNT TWELVE
(Aggravated Identity Theft)**

23. The allegations set forth in paragraphs 1 through 22 of this Indictment are realleged and incorporated by reference.

24. On or about the dates set forth above, within the District of Columbia and elsewhere, Defendants EDWARDS and VENKATA, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, to wit, K.C., during and in relation to certain felony offenses, to wit, Theft of Government Property and Wire Fraud, as alleged in Counts Two through Eleven of this Indictment as set forth above.

**(Aggravated Identity Theft and Aiding and Abetting and Causing an Act to be Done,
in violation of Title 18, United States Code, Sections 1028A and 2)**

**COUNT THIRTEEN
(Aggravated Identity Theft)**

25. The allegations set forth in paragraphs 1 through 22 of this Indictment are realleged and incorporated by reference.

26. On or about the dates set forth above, within the District of Columbia and elsewhere, Defendants EDWARDS and VENKATA, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, to wit, S.B., during and in relation to certain felony offenses, to wit, Theft of Government Property and Wire Fraud, as alleged in Counts Two through Eleven of this Indictment as set forth above.

**(Aggravated Identity Theft and Aiding and Abetting and Causing an Act to be Done,
in violation of Title 18, United States Code, Sections 1028A and 2)**

COUNT FOURTEEN
(Aggravated Identity Theft)

27. The allegations set forth in paragraphs 1 through 22 of this Indictment are realleged and incorporated by reference.

28. On or about the dates set forth above, within the District of Columbia and elsewhere, Defendants EDWARDS and VENKATA, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, to wit, B.U., during and in relation to certain felony offenses, to wit, Theft of Government Property and Wire Fraud, as alleged in Counts Two through Eleven of this Indictment as set forth above.

**(Aggravated Identity Theft and Aiding and Abetting and Causing an Act to be Done,
in violation of Title 18, United States Code, Sections 1028A and 2)**

COUNT FIFTEEN
(Aggravated Identity Theft)

29. The allegations set forth in paragraphs 1 through 22 of this Indictment are realleged and incorporated by reference.

30. On or about the dates set forth above, within the District of Columbia and elsewhere, Defendants EDWARDS and VENKATA, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, to wit, M.C., during and in relation to certain felony offenses, to wit, Theft of Government Property and Wire Fraud, as alleged in Counts Two through Eleven of this Indictment as set forth above.

**(Aggravated Identity Theft and Aiding and Abetting and Causing an Act to be Done,
in violation of Title 18, United States Code, Sections 1028A and 2)**

COUNT SIXTEEN
(Destruction of Records)

31. The allegations set forth in paragraphs 1 through 16 of this Indictment are realleged and incorporated by reference.

32. On or about April 19, 2017, DHS-OIG Special Agents executed search warrants at the residences of Defendant EDWARDS and Patel.

33. On or about April 20, 2017, DHS-OIG Special Agents interviewed Defendant VENKATA at DHS-OIG Headquarters in the District of Columbia. During the interview, Defendant VENKATA was questioned about his contacts and communications with Defendant EDWARDS and Patel, EDS, and whether he had ever provided copies of EDS, or other government software, code, or database data to anyone outside of government.

34. On or about April 20, 2017, Defendant EDWARDS placed five telephone calls to Defendant VENKATA's cell phone.

35. Between on or about April 20, 2017, and April 27, 2017, within the District of Columbia and elsewhere, Defendant VENKATA, with the intent to impede, obstruct, and influence, and in relation to and in contemplation of, the investigation and proper administration of matters within the jurisdiction of departments and agencies of the United States, did knowingly destroy, mutilate, and conceal records and documents, to wit: Defendant VENKATA's text and email correspondence with Defendant EDWARDS and Patel, and which destruction, mutilation, and concealment Defendant VENKATA well knew and contemplated were related to the proper administration of DHS-OIG's investigation of Defendant EDWARDS, Defendant VENKATA, and Patel, a matter that Defendant VENKATA knew and contemplated was within the jurisdiction

of DHS-OIG, a department and agency of the United States, in violation of Title 18, United States Code, Section 1519.

**(Destruction of Records,
in violation of Title 18, United States Code, Section 1519)**

A TRUE BILL:

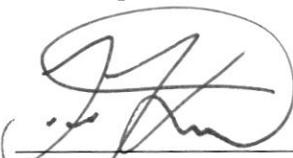
FOREPERSON



ATTORNEY FOR THE UNITED STATES IN
AND FOR THE DISTRICT OF COLUMBIA

Timothy J. Shea
United States Attorney
For the District of Columbia
U.S. Department of Justice

Corey R. Amundson
Chief
Public Integrity Section
U.S. Department of Justice

BY: 

David B. Kent
Assistant United States Attorney
Fraud & Public Corruption Section

BY: 

Victor R. Salgado
Trial Attorney
Public Integrity Section