

**FILED**

**FEB - 2 2016**

Clerk, U.S. District and  
Bankruptcy Courts

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

**UNITED STATES OF AMERICA** :

v. :

**CHARLES HARVEY ECCLESTON** :

**Defendant.** :

**Criminal No. 15-CR- 54 (RDM)**

**STATEMENT OF OFFENSE IN  
SUPPORT OF DEFENDANT'S PLEA OF GUILTY**

The United States of America, by its attorney, the United States Attorney for the District of Columbia, respectfully submits the instant Statement of Offense in Support of Defendant's Plea of Guilty to an Information in the above-captioned matter which charges the defendant with one count of Attempted Unauthorized Access and Intentional Damage to a Protected Computer, in violation of 18 U.S.C. § 1030(a)(5)(A), (b), and (c)(4)(B), and one criminal forfeiture allegation.

*Elements of the Offense*

The essential elements of the offense of Attempted Unauthorized Access and Intentional Damage to a Protected Computer, in violation of 18 U.S.C. § 1030(a)(5)(A), (b) and (c)(4)(B), each of which the government must prove beyond a reasonable doubt to sustain a conviction, are:

- i. The defendant knowingly caused or attempted to cause the transmission of a program, information, code, or command; and
- ii. as a result of such conduct, intentionally caused or attempted to cause damage without authorization to a protected computer.

"Damage" as used in section 1030(a)(5) is defined as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8).

For purposes of Section 1030(a)(5), a "protected computer" is defined by Section

1030(e)(2) to mean a computer: “exclusively for the use of . . . the United States Government, or, in the case of a computer not exclusively for such use, used by or for . . . the United States Government and the conduct constituting the offense affects that use by or for . . . the Government.”

***Penalties for the Offense***

18 U.S.C. §1030(c)(4)(B) provides that a violation, or attempted violation, of Section 1030(a)(5)(A) is a felony punishable by up to ten years of incarceration, “if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i).” one of which is “damage affecting 10 or more protected computers during any 1-year period.” 18 U.S.C. §1030(c)(4)(A)(i)(VI).

U.S. Sentencing Guideline § 5E1.2 permits the Court to impose an additional fine to pay the costs of imprisonment and any term of supervised release and/or probation.

***Factual Proffer***

The following proffer of the government’s evidence is intended only to provide the Court with enough evidence to satisfy the mandate of Rule 11(b)(3) of the Federal Rules of Criminal Procedure. This proffer is not intended to be a disclosure of all the evidence available to the United States nor, to the extent it makes representations concerning statements made by the defendant, is it intended to be a recitation of all that the defendant said.

Had this matter gone to trial, the government’s evidence would have shown, beyond a reasonable doubt, the following facts, among many others:

Charles Harvey Eccleston (“the defendant” or “Eccleston”) is a scientist who was employed in that capacity by the Nuclear Regulatory Commission (“NRC”) and the Department of Energy (“DOE”). During portions of this employment the defendant was granted a security

clearance which allowed him access to information on nuclear energy programs. The defendant left his position at the NRC in 2010. In 2011 he moved to the Philippines where he took up residence.

On or about April 15, 2013, the defendant walked into the embassy of a foreign nation ("Country A") in Manila, Philippines and stated that he had secret United States Government information he wanted to provide to an official of Country A at the embassy. The defendant offered a list of 5,082 email accounts of all officials, engineers, and employees of a United States Government energy agency, which he explained he was able to retrieve because he was an employee of a U.S. Government agency, held a top secret security clearance and had access to the agency's network. The defendant asked for \$18,800 from Country A in exchange for the email accounts. When asked the benefit of obtaining these addresses, the defendant stated they were "top secret" and represented email accounts where official correspondence between officials and employees at the agency was being conducted. When asked what he would do if Country A was not interested in obtaining the U.S. Government information the defendant was offering, the defendant stated he would offer the information to China, Iran, or Venezuela, as he believed these countries would be interested in the information. The defendant provided a contact email and a code to use if Country A wanted to contact and meet the defendant and pay him for the U.S. Government information.

Representatives of Country A subsequently informed the Federal Bureau of Investigation ("FBI") of the defendant's activity described above, after which FBI agents contacted the defendant posing as an intelligence agent for Country A. Through phone calls and email correspondence, the defendant arranged to meet with the person he believed to be an intelligence agent for Country A, but was actually an FBI undercover employee ("FBI UCE1"). During the

meeting, which took place at a hotel in Manila, Philippines on November 7, 2013, Eccleston told FBI UCE1 that, when he worked for the U.S. Government, he had held a top secret security clearance and had worked on top secret United States Government projects. Eccleston told FBI UCE1 he had made previous attempts to sell U.S. Government information to Venezuela and China, but was not granted access to officials of these countries. Eccleston told FBI UCE1 he had made an additional attempt to sell U.S. Government information to the French the day prior to meeting FBI UCE1. Eccleston stated he was successful in meeting with an official from the French Embassy in Manila, and provided the official with his contact information. Eccleston told FBI UCE1 if FBI UCE1 did not get back to him in sixty days with a request for more information, that he would sell U.S. Government information to the French.

During that meeting, Eccleston showed FBI UCE1 a list of approximately 5,000 email addresses he said belonged to NRC employees. Eccleston offered to sell the email addresses and the names of the NRC employees to FBI UCE1 for a total of \$23,000. Eccleston stated that these email addresses could be used to insert a virus onto NRC computers, or to send a large quantity of emails to the accounts to shut down the NRC's servers, and he offered to help FBI UCE1 develop and implement such a plan. Eccleston proposed setting up a conference website and emailing a malicious link to the conference to NRC employees. Eccleston stated that when the link was accessed by the NRC employees, it would download a virus onto the NRC employees' computers that would allow the Government of Country A to track the computer activity of the NRC employees who had accessed the malicious link. Specifically, Eccleston proposed to FBI UCE1:

... Suppose you send out twenty emails. You certainly don't want to send out 4,635 but, but I can even help you target some of the individuals... so because I know a lot of the individuals to target. But let's suppose you send out twenty innocent looking, you build a website and on the website, I know what they're looking for. I know

what their needs are. Okay, and so you build a website and you say in 2014 we are going to have this international conference, and this is what the topics are going to be and they are going to be topics that they want to know about. Okay. And not only that, but we are offering chairmanships to run some of the committees. Well, these people always want to be chairs of important, you know, things, and so you even give them leadership positions and stuff, and you say here, just click here and you'll get in and see the information. You know, when you click that can open it up for a virus. ... You know you setup a conference...you put a website up...they click on the advertisement and whammo now they got a virus. The virus could be monitoring everything they - everything they do in their computer, and then... relaying the information back....

Eccleston also suggested that FBI UCE1 could re-sell the email addresses to Hezbollah.

FBI UCE1 agreed to purchase a thumb drive containing approximately 1,200 email addresses of NRC employees. Later analysis revealed that these email addresses were publically available. Before leaving the meeting, FBI UCE1 provided Eccleston with \$5,000 in exchange for the emails addresses and an additional \$2,000 for travel expenses.

Over the next several months, the defendant corresponded regularly by email with FBI agents still posing as the foreign intelligence operative, regarding the matters discussed at the November 7, 2013 meeting. The defendant eventually planned a meeting with a second undercover employee of the FBI ("FBI UCE2") who had been introduced to the defendant by FBI UCE1 via email some weeks before. On June 24, 2014, Eccleston met FBI UCE2 at a hotel in Manila. At the beginning of the meeting, FBI UCE2 paid Eccleston \$2,000 for his time spent traveling to Manila for the meeting. During the meeting, Eccleston discussed having a list of 30,000 email accounts of all Department of Energy ("DOE") employees which included every DOE scientist and engineer responsible for researching, designing and building U.S. nuclear weapons. Eccleston reiterated the plan to use a list of email addresses as the foundation for a cyber-attack on a U.S. Government energy agency:

...if somebody really wanted to get pissed off, they could do a denial of service to 30,000 employees. You could also send messages – for example, you could put up an innocent looking website that says we're holding a conference in such-and-such a country. The conference will cover such-and-such a subject, which would be high interest to those people. And then, use it to your advantage. You know there's lots of ways this could be done...

Eccleston also told FBI UCE2: "If we make a mistake, I'm going to be locked up for the rest of my life."

During the meeting, the defendant and FBI UCE2 agreed that the defendant would pursue the general scheme that he had set forth, and the FBI UCE 2 would pay the defendant \$1,000 for each recipient to whom Eccleston eventually sent the infected emails.

On or about July 30, 2014, Eccleston sent two documents to the FBI undercover agent via a cloud-based file service under a fictitious name. The documents, created by Eccleston, included a table titled "Comparative Assessment of Advantages and Disadvantages of Selected Scientific Conferences (2014-2015)," and instructions on how to read the table. The table contained descriptions and links to nine real websites identified by Eccleston that referred to nuclear-related conferences that would occur in the coming year, and Eccleston's assessment of the advantages and disadvantages of the use of each conference as a lure to target DOE employees in furtherance of the proposed scheme. In an accompanying document, Eccleston stated:

...I researched scores of different scientific conferences that would be of interest to the targeted audience. I narrowed it down to nine conferences ...I believe a list of 100 addresses is about the right number. Its [sic] not too large to attract attention, yet its [sic] large enough to generate sufficient interest and "clicks" from those reading the email... Most email (yahoo, MSN, AOL etc) providers place a maximum restriction on the number of messages that can be sent in a single day. Therefore, we may want to send our email using 3 or 4 different email accounts (33-25 recipients from each email account). This would further reduce any undue scrutiny or

attention... we might also want to send two different conference announcement emails. This would allow us to target a more diverse audience and would again reduce any undue scrutiny or attention...

On or about September 12, 2014, the defendant sent documents to the FBI undercover agent through a cloud-based file service, again using a fictitious name. One of the documents, titled "Department of Energy List of Recipients," contained a chart including the names, email addresses, and identified positions of 55 DOE employees. Also included in the document was a section titled "Selection Rational," which included Eccleston's written assessment of the type of "privileged" information to which the listed individuals had access. Therein, the defendant made specific reference to individuals with "unrestricted access to information about "N-wpns" and "N-materials," - coded references to nuclear weapons and nuclear materials.

On or about September 19, 2014, the defendant sent two more documents to the FBI undercover agents via a cloud-based file service. One of the documents titled "Email & Website Announcement" contained what appeared to be two PowerPoint slides advertising an upcoming 2015 conference sponsored by a nuclear society based in Washington, D.C. One of the advertisements included a small yellow rectangle on the lower right hand side of the slide. Inside the rectangle was the following statement: "Conference details and registration: (\*\*Icon to click on\*\*)."

The accompanying document, entitled "Advertisement instructions," stated, in part:

... The first page is the draft for the email that will be sent to the 50 customers.

If I correctly understand Phase 4, two links will be placed in the email announcement for the customers to click on. The links would be placed in the small yellow rectangle on the lower right hand side of the email announcement...

The defendant's planning continued, and, in early January 2015, he requested that the FBI undercover employee provide him with the link which, according to their discussions, the defendant believed would contain malicious computer code and which he would plant into the email he had drafted. On January 15, 2015, the defendant sent slightly differing versions of the email he had drafted, containing the link he had received from the FBI undercover account above to approximately 80 employees of the Department of Energy. The email advertised a conference focused on nuclear topics, education and training. The defendant believed that the emails contained a link which, if activated by the recipient, would release a malicious virus into the DOE computer system. Unbeknownst to the defendant, the link was benign. The defendant believed he would be paid approximately \$80,000 for this activity by representatives of Country A.

A consensual search of the DOE servers confirmed that the defendant's email was sent to intended recipients having offices located in Oak Ridge National Laboratory in Tennessee, Los Alamos National Laboratory and Sandia National Laboratory, both located in New Mexico, and Lawrence Livermore National Laboratory, located in California, as well as Department of Energy offices in Washington, D.C.

Respectfully submitted,

CHANNING PHILLIPS  
UNITED STATES ATTORNEY  
D.C. Bar # 415793

BY:



THOMAS A. GILLICE  
Assistant United States Attorney  
D.C. Bar # 452336  
555 4<sup>th</sup> Street, NW  
Washington, DC 20530  
202-252-1791



***Defendant's Acceptance***

I have read or had read to me the \_\_\_ pages which constitute the government's Statement of Offense and have discussed it with my attorney. I fully understand this proffer and agree to it without reservation. I do this voluntarily and of my own free will, intending to be legally bound. No threats have been made to me nor am I under the influence of anything that could impede my ability to understand this agreement fully.

I reaffirm that absolutely no promises, agreements, understandings, or conditions have been made or entered into in connection with my decision to plead guilty except those set forth in my plea agreement.

I am satisfied with the legal services provided by my attorney in connection with this proffer and my plea agreement and matters related to it.

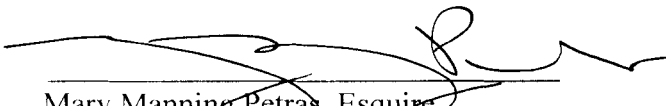
Date: 2-2-16

  
\_\_\_\_\_  
CHARLES HARVEY ECCLESTON  
Defendant

***Attorney's Acknowledgment***

I have read each of the \_\_\_ pages which constitute the government's Statement of Offense, reviewed them with my client, and discussed the provisions of the proffer with him, fully. These pages accurately and completely set forth the government's proof as I understand it.

Date: 2-2-16

  
\_\_\_\_\_  
Mary Manning Petras, Esquire  
Attorney for  
CHARLES HARVEY ECCLESTON