IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	
V.	:	CRIMINAL NO. 16-481
ADAM FLANAGAN	:	

GOVERNMENT'S CHANGE OF PLEA MEMORANDUM

The defendant has agreed to plead guilty to Counts Nine and Ten of the Indictment, charging him with violating 18 U.S.C. § 1030(a)(5)(B), intentionally accessing a protected computer without authorization and as a result of such conduct, recklessly causing damage. The government submits this memorandum to the Court to outline the plea agreement, to give a factual basis for the plea, and to list the elements of the offense and the penalties.

I. THE PLEA AGREEMENT

The defendant will plead guilty to the Counts Nine and Ten of the Indictment, charging a violation of 18 U.S.C. § 1030(a)(5)(B). At the time of sentence, the government will dismiss the remaining counts of the Indictment. The defendant agrees to forfeit the computer that he used to commit the offenses. The parties have also agreed upon certain Sentencing Guidelines calculations. The stipulations involve the base offense level, the fact that the crime involves a special skill and/or an abuse of trust, and the fact that the defendant has accepted responsibility. The parties have not reached an agreement on the amount of loss to the victim, which is part of the calculation of the Offense Level.

The agreement also contains standard terms regarding the waiver of the right to appeal or bring a collateral attack on the conviction (preserving the right to raise issues of the effectiveness of counsel.)

II. STATEMENT OF FACTS IN SUPPORT OF THE GUILTY PLEA

Adam Flanagan lived in Bala Cynwyd, PA, and worked for a North Carolina-based company. The company's name is known to the government and can be disclosed to the Court. For the purpose of public filings, the government will refer to it as it did in the Indictment as "Company A". Company A built Tower Gateway Base stations (TGBs) which provided monitoring of utility usage of residences. The TGBs in this case were all designed to gather data from residential water meters. The TGB would be mounted on a pole and would receive radio signals from residential water meters. This allowed for billing without sending a meter reader into a home. It also allowed the provider of the water to aggregate data about water usage in the district.

Flanagan was hired by Company A on December 3, 2007 as a Radio Frequency Field Engineer. He worked on the team that installed TGBs. In his March 31, 2013 annual performance review, he was rated "below expectations." On June 4, 2013, he was placed on a performance improvement plan. He completed the plan with only modest improvement on September 23, 2013. On October 22, 2013, he signed a separation agreement with Company A, effective November 16, 2013. Over the next several months, TGBs that Company A had provided to a number of municipalities developed problems.

KENNEBEC WATER DISTRICT

The first incident occurred on December 10, 2013, when the Kennebec (Maine) Water District was unable to connect to its TGBs. Flanagan had installed the Kennebec TGB on

June 17, 2013. (No one checked these devices logs until February 2014, so they did not capture the intruder's IP address. Therefore, it is not possible to attribute this attack to anyone).

Thereafter, on March 1, 2014,[1] an entry was made to the Kennebec TGB by entering the default root password.[2] The intruder changed the communication channel frequency, thus disabling the tower's ability to transmit information to the Remote Network Interface (RNI). (As a Radio Frequency Field Engineer, Flanagan's job was to set the radio frequencies on which the TGBs communicated when they were installed.) The RNI receives data from and communicates with the TGBs across the network and processes the data however the utility sees fit. The IP address for the intruder was 50.11.223.159. That IP address belongs to Clearwire. Clearwire is now part of Sprint and it has identified the tower location for that IP address in Lower Merion Township, about 1 mile from Flanagan's residence.

On April 30, 2014, there was another intrusion into the Kennebec TGB from IP address 50.11.223.159. The default root password was used to log in and the radio frequency for communications was changed, disabling the tower.

The Clearwire records for IP address 50.11.223.159 show that it was assigned to Flanagan from at least April 1, 2014 through August 1, 2014. The records show no other

[1] The facts regarding actions on dates involving the same water authorities, but which are not the dates on which the crimes to which the defendant is entering his plea, are set forth as relevant conduct under § 1B1.3(a)(a)(A).

[2] When Company A installed TGBs there was a password already created. It was not particularly complicated and known to the Company A personnel performing the installation. Customers were told to change the password when they started operations. A number, including the Kennebec Water District failed to do so.

person assigned during this time and each assignment recorded the MAC address[3] of Flanagan's WiMax modem. Clearwire examined its IP assignment logs, looking at the MAC addresses of the devices to which this IP address was assigned during this time, the only MAC address in the logs was the one belonging to Flanagan's WiMax modem. (The agents seized that modem when they executed a search warrant of his home on September 4, 2015.)

SPOTSWOOD, N.J.

On May 4, 2014 there was a successful intrusion into a Spotswood TGB from IP address 50.11.223.159, using the default password. The intruder changed the password to "fuckyou."[4]

DEFENDANT'S STATEMENTS

Flanagan was interviewed three times by the FBI. Each time the agents surreptitiously recorded the interview. The first interview occurred on the night of September 4, 2015. The agents had executed a search warrant on Flanagan's apartment that morning. Flanagan was not home. The agents learned that he was out of town and returning by airplane that evening. They met him at the airport shortly after 10 PM to talk to him and to execute a warrant for his person to seize any computers or digital storage devices. In the course of the interview, Flanagan said a

[3] A MAC (media access card) address is a hard-wired serial number given to any network connecting device, such as a wireless card or an Ethernet card. It uniquely identifies the device.

[4] The Aliquippa (Pennsylvania) Water Authority had similar problems. Those facts are not offered to support the guilty plea, but since they are relevant conduct for the purposes of calculating the Sentencing Guidelines (§ 1B1.3(a)(1), I set them forth here.

> On April 3, 22, 24, and 28, 2014, there were multiple intrusions into one of the Aliquippa Water Authority's TGBs. All the intrusions were made from IP address 50.11.223.159. On one of the intrusions on April 22, the intruder changed the radio frequency for communications. He also changed the code for a computer script to the lyrics of a Pink Floyd song.

number of things about his conduct, which are excerpted below. (AP = S/A Andrew Pelczar; DM = S/A Darin Murphy; AF = Adam Flanagan)

AP: What did you do it? How'd you do it?

AF: It…you would just log on…

AP: Like from your home…

AF: Yeah through a proprietary program. Yeah.

AP: Alright. So from your home computer you would dial in…

AF: Well I worked from home. So I would

AP: So you were always there.

AF: It was always there…so I had…It was on my computer so when they let me go. It was still there.

AP: I mean I have had other cases like this and what will happen guys will have a couple of beers….

DM: That's….

AP: Get a little loose

AF: Pretty much.

AP: You got pissed and had a couple.

AF: Pretty much yeah.

AP: Alright. Alright.

DM: That's very different than you being this master hacker who is trying to take down…

AF: I am not at all a master hacker.

DM: But that's why we are here because you look on paper and here's somebody who's…

AP: You have skills…

DM: Methodically logging in…

AF: Not really. No I don't…

AP: On paper you do.

AF: That's not. That's absolutely not true.

AP: So. Alright.

AF: I'm an RF guy, I know rudimentary ah logon. A couple of VI scripts. I knew the entrance screen was to do a VI. You know you can do a VI and it gave you a welcome message. So a couple of times I changed the root welcome message to say, "Ha. Ha."

AP: Like obscenities or something.

AF: I don't know. I don't think so. I don't know…maybe. Um. ASCII pictures. Just a couple of ASCII pictures. Um.

AP: Okay. Just, like to deface it. Fuck with them.

AF: Pretty much. Yeah.

AP: Alright, Um.

AF: Like I say. I am honestly at fault but yeah it was nothing to be, I don't want to say it wasn't being malicious but it wasn't anything to, you know, take down a network like that (UI)

Transcript of 9/4/15, pp. 11-13.

AF: They let me go. Yeah.

AP: Why did they let you go?

AF: Um. It was my, they, I, it's more. I think it was more internal fighting between the different groups in Company A.

AP: Okay.

AF: Ah. There was a lot of internal fighting in Company A I thought.

AP: Okay.

AF: So um…

DM: So your motivation was just…

AF: Just to fuck with them. I mean it was absolutely…

DM: You're not doing this type of activity towards any other company?

AF: I don't even have that remote type of skill. I mean that's…

DM: Okay.

Transcript of 9/4/15, p. 16.

AP: We are trying to figure it out and this is helpful. And we appreciate you taking time out of getting home or wherever you're going to talk to us. Um. So you used the laptop to do it that you no longer have and you used a hotspot to do it. Where the hotspots?

AF: Ah na. I didn't use a hotspot?

AP: Or WIFI. What did you do?

AF: Either my home network at the time or ah…

AP: Is that still there?

AF: It was either. I had a Verizon card. That I ah used to use a lot.

AP: Is it air card?

AF: Yeah. Air card. It was just simple. It was just a simple (UI)

Transcript of 9/5/15, p. 18.

AP: And you left Company A. When did you say earlier?

AF: October 2013.

AP: That would be within some period of time after that that you did this.

AF: Right after.

AP: Within weeks, months?

AF: Weeks. Weeks.

AP: Alright. Alright. Alright.

AF: But as far as I can remember it was weeks. Ah.

AP: Okay.

AF: I don't know if that was exact but definitely you know when I took another job I was like whatever. There's no…

AP: Clean slate. Just a…You were done.

AF: Yeah, like I, I wasn't being malicious. I was just very annoyed at one of the persons that worked there.

AP: Who was that?

AF: Mike Gaston.

AP: Was he a manager or something?

AF: He was.

AP: Was he the one you think was responsible for cutting you lose.

AF: Ah. I don't…He did not like me at all for some reason. I don't know.

AP: Is he a Raleigh guy? Or was he up here?

AF: He's a Pittsburgh guy.

AP: Pittsburgh guy. Okay. But he was the guy you reported to?

AF: He was yes. He took over (UI) Yeah.

AP: Okay. So you guys had some friction or he had an issue with you?

AF: He had an issue with me.

AP: Alright. And that led to you making this decision.

AF: Coming home drinking after a few beers.

AP: And loggin in.

AF: Loggin in saying these mother fuckers.

DM: And would he be the guy who had to deal with this situation then?

AF: Probably.

AP: Would it be his mess to clean it up.

AF: I don't know. I mean. Like I said. I don't think it was a mess to clean up. That much of a mess but it was a….

AP: I mean somebody had to fix it.

AF: Yeah. It would have to be he (UI)

AP: So it would be his thing to fix. Alright. Kind of a, little FU to him. Would you think he thought you would do it? Or? Were you not worried about it?

AF: I don't know. I don't know. The times I did like I said were like coming home from the bar, drinking, (UI) making very stupid decisions.

DM: But that changed since. You tell us, you know…

AF: As far as a master hacking ring. That's insane. That is…I mean I wish I had that skill.

AP: Well that's why we are talking to you because we need your help to figure this out.

DM: Yeah. We don't know unless, you know…

AF Like I said. I wish I had that skill. That is by far…I was the RF guy doing the wireless metering data (UI) but as far as a master hacker that's insane.

DM: Ok. Alright.

Transcript of 9/4/15, pp. 19-21.

The agents then executed the search warrant on Flanagan's person. As the interview wrapped up, the following occurred.

AP: Any questions?

AF: I mean. What am I looking at? That's what I don't…

AP: We don't know. You call me next week and we'll figure it out after we get a chance to go over everything. We'll know more.

AF: Is there somebody I could like…

AP: Well let me ask you, let me turn that… What haven't you told us?

AF: That's…I told…I mean. I logged on. Change some, you know, change the scripts of a couple of them. Put a picture of them. I think I put a pirate picture on one. Changed a few scripts to say some stupid stuff. But other than that. I don't think I changed anything. Terribly. I mean. Nothing that they couldn't go and say….

DM: You pretty sure you didn't change the root password or the default password.

AF: I don't think. I mean I don't…

AP: See. We think you did.

AF: I don't think I did.

AP: But we think you did. And it's very important for us to think that you didn't but we think you did right now.

AF: Ah. I…

AP: Because that's where additional damage occurred and we believe strongly that you changed that root password. And we appreciate you being candid. I know it's uncomfortable to own up to stuff that you did when you were, when you had a beer or two, and you were pissed at your employer. But we think strongly that you changed…We think we can prove that you changed that root password. So I don't wanta…

AF: I don't know if I did or not. I may have. I don't know.

AP: You may have.

AF: I may have. I don't know. Possibly.

AP: Possibly. Probably, possibly?

AF: I don't know man. I could have.

AP: Okay. Because remember the candor is….

AF: I mean. I don't remember exactly what I did. I remember I was getting them. I was doing a lot of stuff. If you're saying I did. I probably did.

AP: Well I am asking. But we believe it happened and we think, we believe we can prove it came through your network.

DM: That doesn't make it any better or worse. We're not…

AP: We are just trying to get to the truth.

DM: What's more important is the truth.

AF: Yeah. I mean. I changed. I may. I don't know to be honest. I…

AP: Because changing the root password is different than defacing the site. Two different things and I am trying to figure out what you recall doing.

AF: If I changed it, it wasn't, I don't know. I may have. I don't know. I don't. It's possible (UI). If you said I did. I probably did.

AP: Oh. I am not trying to put words in your mouth but I am saying that we have logs and other things that make us feel strongly that you did it. And we had to search your house. And so, a judge believed that our information was, was convincing enough for probable cause that you did it.

AF: Yeah. Alright. Then that's the case. I probably did then. I didn't do it to…

AP: I'm not trying to put words in your mouth. I am just trying to have you tell us the truth the best you could recall.

AF: I didn't go in and…You know, I was just going in there cause like I was pissed. I was extremely angry. I don't specifically remember, remembered what I changed. I remember putting pictures in, changing scripts, a few scripts. Passwords maybe. If you said I did it. I probably did it.

AP: Okay. Okay. Well.

DM: You have the weekend. Think about it. (UI) If you think of something else...

AF: As far as, that's the only thing I know how to do. Was ah, change file names, change scripts.

AP: But here is what's going to happen. You are gonna go home and you're going to go to bed and you're going to lie in bed and have a hard time falling asleep. And you're going to start remembering everything with a little more clarity because you are thinking about it. When we talk on Tuesday. I am going to ask you some of the same questions and ask you if you recall doing things like the root password. Do you best to try to remember over the weekend what you did and what you didn't do…?

AF: When you're saying the root password?

DM: The admin password and login whatever, whatever how it is set up in the system.

AF: To the TGB?

DM: Yeah.

AF: I probably. They, we changed them quite a bit. Or I did. Umm. When I worked there I changed them.

DM: Right.

AF: So. That probably was changed then. Cause that's….

AP: After you were fired?

AF: Probably. Yeah. Yeah.

AP: Do you remember doing it specifically? Like sitting her in that chair, hanging out with us.

AF: I could not tell you what sites I went on. I had them on a list. I had um, Telnet set up my computer.

AP: You had what on your computer?

AF: Telnet, um Telnet program. And I had all the site names that I could just go in and it would just connect automatically.

Transcript of 9/4/15, pp. 59-62.

The agents seized a number of items from Flanagan on September 4 that his new employer had issued to him. They met him again on September 8 to return these items and to talk to him again. Once again they surreptitiously recorded the conversation, excerpts of which are set forth below.

AP: I mean here's, here's what I wanted to finish talking with you about is, I mean you told us Friday night that you um, you got in, into their system and you, you defaced it by putting the different pics on (UI). I get that. I get that.

AF: I may have changed the password to "fuck you" on a couple of them. I don't, I…

AP: The root password?

AF: I don't know.

AF: The password, password. When you log on, is that the root password? I don't know.

DM: Yeah, that's the one you use when to log in to the system.

AF: Maybe. I don't remember. I, which one I did it, I mean it wasn't, I didn't sit there and keep a log to say on this date I did this.

DM: Um. Were all of them on the same night?

AF: No.

DM: It was over a few nights period?

AF: Probably (UI) quite a few times.

DM: Yeah.

AF: When, when where and how, which sites they were I couldn't tell you.

DM: I mean, we have it, I just didn't remember if it was all in one night. (UI) bunch of stuff. Yeah, it's all in the logs.

AF: Oh.

AP: I don't know off hand how many times it was either, but like I said.

AF: No, I (UI).

AP: I know it was more than once.

Transcript of 9/8/15, p. 5.

AP: Yeah, but, but, but did you know, I mean, you're fired. You're not supposed to go back in the system right? I mean, you're fired. Correct?

AF: Yeah.

AP: I mean, you know that, right?

AF: Yeah.

AP: When you get fired you're not supposed to do that.

AF: Yeah, I know that. I honestly, the, I know I wasn't supposed to be there. I, what I, I was doing it more to just to be a dickhead.

AP: Okay.

Transcript of 9/8/15, pp. 11-12

AP: How would you fix what you did if you did it yesterday? Do you know how to fix what you did?

AF: Ah I guess. I…Not anymore. Like I said. I've been through a bunch of training when I worked there I probably could have.

AP: Okay.

AF: You know. Just go in and change the password again and ah...just rearrange some scripts.

AP: OK. So it that what you did in your apartment? Scripts and passwords?

AF: I made them. I don't know the passwords. I may have. If I said I did. I…

AP: But you haven't said you did it yet. That's why I am trying to learn.

AF: Yeah if I did it…

AP: Because I think you did.

AF: If I did. I don't know. Um…

AP: What about scripts?

AF: Scripts. Probably change some, you know, I know basic VI.

AP: Do you remember doing that though?

AF: I don't. I mean.

DM: Well how would you alter the scripts? Like what would you…

AF: Like you would do VI. If the script was there...

DM: Yeah you go into VI.

AF: If the script was there you would do VI and where it said this does this...

DM: You would change it.

AF: Fuck you. Whatever. Then.

DM: Yeah. Okay. Alright.

AF: Stupid shit like that.

DM: And so when you change the scripts, so I'm clear. You would change on the comments sections..or?

AF: I don't, I don't, you know like I said. I was just banging it in there. What exactly... I couldn't tell you.

AP: Do you remember changing the passwords to these mobile based stations?

AF: I don't remember. I mean if…if it.

AP: I mean there is a lot of them.

AF: If I did it. Nah I didn't…The only thing (UI) I may have changed a few.
I don't remember. Like I said. I don't remember off hand
Transcript of 9/8/15, pp. 22-24

III. ELEMENTS OF THE OFFENSE

Section 1030(a)(5)(B) has both "conduct" elements and "result" elements. Section 1030(a)(5)(B) provides as follows:

> Whoever intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage.

The government must prove that the defendant committed the following conduct elements:

i) Accessed a protected computer without authorization

ii) As a result of the unauthorized access

iii) Recklessly caused damage

Since Flanagan no longer worked for Company A and because Company A did not operate the TGBs for the water districts in any event, Flanagan was not authorized to access them. *United States v. Steele*, 595 F. App'x 208 (4th Cir. 2014) (once an employee leaves a

company, he is no longer authorized to access its system, even if his password still works); *United States v. Shahulhameed*, 629 F. App'x 685 (6th Cir 2015) (same); *United States v. Nosal*, 844 F.3d 1024 (9th Cir. 2016) (former employee who uses current employee's credentials to access the system, even with the permission of the current employee is making an unauthorized access).

The mental state for the access is "intentionally." The Third Circuit has held that the term "intentionally" means "performing an act deliberately and not by accident." *United States v. Carlson*, 209 Fed. Appx.181 (2006) (construing this section); *United States v. Barbosa*, 271 F.3d 438, 457 (3d Cir. 2001) (in the drug context, cited with approval in *Carlson*). *See also Pulte Homes v. Laborers International Union*, 648 F.3d 295, 303 (6th Cir. 2011) (citing *Carlson*)

The mental state for causing damage is "reckless." To show recklessness the government must show that the defendant was "aware of the facts from which the inference could be drawn that a substantial risk of serious harm exists, and he must also draw the inference." *Farmer v. Brennan*, 511 U.S. 811, 837 (1994); *Natale v. Camden County Correctional Facility*, 318 F.3d 575, 582 (3d Cir. 2003). The test is subjective, not objective – the defendant must actually be aware of the facts and from them, draw the inference that the risk exists.[5] It is not enough to show that a reasonable person would do so.[6] Since the

[5] *See also United States v. Johnstone*, 107 F.3d 200, 208, n. 9 (3d Cir. 1997):

> Moreover, reckless disregard often entails some form of indifference. *See, e.g., Black's Law Dictionary* 1270 (6th ed. 1990) ("For conduct to be 'reckless' it must be such as to evince disregard of, or indifference to, consequences...."). In common parlance, for an individual to be indifferent, he must not be concerned "one way or the other" about the consequences of his action. *Webster's Third New International Dictionary* 1151 (1966).

Footnote continued on following page.

changing of a passcode or radio frequency or the replacement of computer code with song lyrics would clearly be intentional acts, the government would have no problem proving the element of recklessness.

The term "damage" is defined in § 1030(e)(8) as "any impairment to the integrity or availability of data, a program, a system, or information." By changing the radio communications frequencies and overwriting computer scripts, Flanagan impaired the availability of the TGB system to perform. By changing the password, he impaired the ability of the rightful owner to access the TGB.

Under 18 U.S.C. § 1030(e)(1), the term "computer" means:

> an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

A "protected computer" is defined in § 1030(e)(2)(B) as one that "is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce

---

> A requirement that an individual know the consequences of his action is not antithetical to this definition of indifference, but it would introduce an additional element beyond lack of concern.

[6]The *Farmer* opinion cites § 2.02(2)(c) of the Model Penal Code. Compare, 18 Pa. C.S.A. § 302(b)(3):

> A person acts recklessly with respect to a material element of an offense when he consciously disregards a substantial and unjustifiable risk that the material element exists or will result from his conduct. The risk must be of such a nature and degree that, considering the nature and intent of the actor's conduct and the circumstances known to him, its disregard involves a gross deviation from the standard of conduct that a reasonable person would observe in the actor's situation.

or communication of the United States." Since these computers were accessible over the Internet, they were used in and affecting commerce.

The result elements for § 1030(a)(5)(A) are found in the penalty section, and are set forth in § 1030(c)(4)(A). The only one that applies is § 1030(c)(4)(A)(i)(I): causing loss[7] to 1 or more persons during any 1-year period aggregating at least $5,000 in value. Here the cost of just the forensic examination of the Spotswood TGB was $22,500.

IV. MAXIMUM PENALTY

The maximum penalty for a violation of 18 U.S.C. § 1030(a)(5)(B) is 5 years (18 U.S.C. § 1030(c)(4)(A), a $250,000 fine (18 U.S.C. § 3571(b)(3)) and a $100 special assessment (18 U.S.C. § 3103(a)(2)(A)). This is a Class D felony (18 U.S.C. § 3559(a)(4)) and carries a maximum term of supervised release of three years. (18 U.S.C. § 3583(b)(2)). The total maximum penalty would be 10-years' imprisonment, a 3-year period of supervised release, $500,000 fine, and a $200 special assessment. Full restitution and forfeiture of all facilitating property also may be ordered.

Respectfully submitted,

LOUIS D. LAPPEN
Acting United States Attorney

/s/ Michael L. Levy
MICHAEL L. LEVY
Assistant United States Attorney
Chief, Computer Crimes

[7] The term "loss" is defined in § 1030(e)(11) as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the government's Change of Plea Memorandum upon the following by electronic mail:

Douglas Earl, Esquire
1015 Chestnut St.
Suite 902
Philadelphia, PA 19107

/s/ Michael L. Levy
MICHAEL L. LEVY

March 1, 2017