UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

UNITED STATES OF AMERICA,	)	
	)	
v.	)	No. 3:08-CR-142
	)	Judges Phillips/Shirley
DAVID C. KERNELL,	)	
a/k/a "rubico,"	)	
a/k/a "rubico10,"	)	
	)	
Defendant.	)	

UNITED STATES' SENTENCING MEMORANDUM

COMES NOW the United States, by and through its undersigned counsel and hereby respectfully submits its Sentencing Memorandum in this case. For the reasons set forth below, under the applicable Sentencing Guidelines and Section 3553(a) sentencing factors, the government recommends a sentence of 18 months, the middle of the sentencing range.

I. Background

This case involves defendant David Kernell's unauthorized access to the e-mail account of Sarah Palin on September 16, 2008, while she was the Governor of Alaska and the Republican nominee for Vice President, and his destruction of records in anticipation of a federal investigation. Based on evidence presented at trial, the defendant targeted her account with the hope of finding "incriminating" information and to "derail" a national election only seven weeks before the election. In explaining why he had "hacked" into the account, he expressly stated his motive:

> I read though the emails… ALL OF THEM… before I posted, and what I concluded was anticlimactic, **there was nothing there, nothing incriminating,**

> **nothing that would derail her campaign as I had hoped**, all I saw was personal stuff, some clerical stuff from when she was governor…. And pictures of her family … I read everything, every little blackberry confirmation… all the pictures, and there was nothing …

Gov't Exhs. 1, 559, 560 (emphasis added).

After practicing the password recovery process on his own Yahoo! account, the defendant changed and reset the password to the Gov.Palin@yahoo.com e-mail account. By doing so, he established exclusive control over the account and deprived the account holder of access to the account. He then read, copied and disclosed the confidential and personal information in the account on the Internet. As a result of the defendant's actions, the contents of the account were posted on 4Chan, Wikileaks, Photobucket, Gawker, and many other Internet sites and media outlets. *See* Gov't Exhs 2-13 (Photobucket), 14-24 (Wikileaks), 27 (Gawker). Once the information was released on the Internet, the Governor's contacts began receiving numerous unsolicited messages, many of them crude and vulgar. The defendant then decided to share the password he created with others, providing them with the means to intrude into the account. Within minutes, numerous individuals in the United States and around the world accessed the Governor's account. The defendant then bragged to his friends and others about how he had "hacked" into the account.

The defendant received multiple warnings that his actions had been reported to the Federal Bureau of Investigation (FBI) or that the FBI was investigating his conduct, including before he made the decision to share the account password he created. In contemplation of an investigation by law enforcement authorities, the defendant removed, altered, concealed and covered up records and files on his laptop computer relating to his use of, and his establishing control over, the e-mail account of Governor Palin.

The trial commenced on April 20, 2010. Ten days later, the jury found the defendant guilty of obtaining unauthorized access to a protected computer, the lesser included offense under Count Three of the Superseding Indictment, and found the defendant guilty of destroying records, under Count Four. The jury acquitted the defendant on committing wire fraud, Count Two, and was unable to reach a unanimous verdict on identity theft, under Count One. The Court declared a mistrial on Count One, under Fed. R. Crim. P. 26.3, after the jury informed the Court that it was unable to reach a unanimous verdict on Count One, and the Court found a manifest necessity for the mistrial since the jury was hopelessly deadlocked.

II. Maximum Penalties And Sentencing Guidelines Calculations

A. Maximum Penalties

The maximum penalties for Count Three, Fraud and Related Activity in Connection with Computers, in violation of 18 U.S.C. § 1030(a)(2)(C), are as follows:

a.	Maximum prison sentence	1 year
b.	Maximum fine	$100,000
c.	Maximum supervised release term	1 year
d.	Mandatory special assessment	$25

The maximum penalties for Count Four, Destruction, Concealment of Records With Intent to Impede Federal Investigation, in violation of 18 U.S.C. § 1519, are as follows:

a.	Maximum prison sentence	20 years
b.	Maximum fine	$250,000
c.	Maximum supervised release term	3 years

d. Mandatory special assessment $100

B. Applicable Sentencing Guidelines

The following Sentencing Guidelines apply:

a. Count Three: 18 U.S.C. § 1030(a)(2)(C) (Fraud and Related Activity in Connection with Computers)

i. Base Offense Level, U.S.S.G. § 2B1.1(a)(2) 6

ii. Intent to Obtain Personal Information / Unauthorized Public Dissemination of Personal Information, U.S.S.G. § 2B1.1(b)(15) +2

iii. Official Victim, U.S.S.G. § 3A1.2(a) +3

iv. Obstruction of Justice, U.S.S.G. § 3C1.1 +2

b. Count Four: 18 U.S.C. § 1519 (Destruction, Concealment of Records With Intent to Impede Federal Investigation)

i. Base Offense Level, U.S.S.G. § 2J1.2(a) 14

c. Grouping of Closely Related Offenses
Under U.S.S.G. § 3D1.2(c), resulting base Offense Level 14

d. Total Adjusted Offense Level
(Assuming U.S.S.G. § 3E1.1 applies) 14

Based on the foregoing, under the Sentencing Guidelines, a Criminal History I, and Offense Level 14 results. Under the Sentencing Guidelines, a sentencing range of 15 to 21 months results. Consistent with the Sentencing Guidelines, the government respectfully submits that a mid-range sentence of 18 months in prison is consistent with the statutory purposes of sentencing. See 18 U.S.C. § 3553(a) (setting forth relevant sentencing factors such as seriousness of offense, just punishment, adequate deterrence, and protection of public, which are discussed further below).

IV. Consideration Of The Section 3553(a) Factors

As set forth below, the application of the sentencing factors enumerated in 18 U.S.C. § 3553(a) supports the requested imprisonment in this case. The Section 3553(a) factors include:

(1) the nature and circumstances of the offense and the history and characteristics of the defendant;
(2) the need for the sentence imposed –

(A) to reflect the seriousness of the offense and to promote respect for the law, and to provide just punishment for the offense;
(B) to afford adequate deterrence to criminal conduct;
(C) to protect the public from further crimes of the defendant; and
(D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner;

(3) the kinds of sentences available
(4) the kinds of sentences and the sentencing range established in the guidelines . . .
(5) any pertinent policy statement . . .
(6) the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct; and
(7) the need to provide restitution to any victims of the offense.

a. Nature And Circumstances Of The Offense

Under Section 3553(a)(1), the nature and circumstances of the offense strongly demonstrate the need for the requested prison term. In this case, there are two primary aspects to consider concerning the nature and circumstances of the offense. The first is the series of cumulative, aggravating choices made by the defendant in committing the charged crimes. The second is the consequences of the defendant's conduct on the victims and the intended impact of his actions.

1. Eleven Key Decision Points: Aggravating Choices

As established at trial, the defendant's actions were not the result of a sole decision to "hack" into the account but the product of at least eleven key decision points (summarized

below). At each decision point, the defendant could have stopped or at least taken steps to mitigate the harm caused by his preceding actions. Each time he came to a decision fork in the road, instead of mitigating his conduct, the defendant deliberately and consciously selected the path which exacerbated the harm. The decision points, summarized below, include:

(i) Initial Practice and Access
(ii) Initial Review, Exit and Return
(iii) Using A Proxy
(iv) Reading, Copying and Saving Images and Content
(v) Contemporaneously Telling Others About The Hack
(vi) Emailing "i am god" Message
(vii) Disregarding FBI Warnings
(viii) Enabling Further Intrusions
(ix) Bragging About "Hacking" Activities
(x) "Tell[ing] The Story" On 4Chan
(xi) Destroying Records

(i) First Decision Point: Initial Practice and Access

The first key decision the defendant made was to, as the defendant described it, "hack" into the Governor's Yahoo! account. As part of his preparation, on September 15, 2008, around 11:27 p.m. EDT, the defendant conducted a Google search for "jueau zip code". *See, e.g.*, Gov't Exhs. 151, 606. Just after midnight on September 16, 2008, defendant Kernell practiced changing passwords on his own account, Rubico1337@yahoo.com. Gov't Exh. 514.

Once he was familiar with the Yahoo! password recovery process, the defendant decided to use the same process to reset the password on the Gov.Palin@yahoo.com account. In order to answer the security questions on this account, the defendant researched the possible answers using the Google search engine.[1] Ultimately, the defendant changed the account password to

[1] Some of the Google searches traced to the defendant included: ""alaska postal codes," "alaska zip codes," "palin yahoo acct," "palin meet todd spouse," "palin husband," "palin husband meet," "palin husband elope," and "how did palin meet her husband." *See* Gov't Exhs.

"popcorn." *See* Gov't Exhs. 515, 520, 527, 540.

At this point, the defendant had exclusive control and access over the account.[2] Even the account holder could not access her own account without the new password.

(ii) Second Decision Point: Initial Review, Exit and Return

After compromising the account, the defendant began to review the contents. After less than two minutes in the account, the defendant exited. After leaving the account, the defendant had a second key decision to make. He had already seen some of the contents in the account. What should he do next? Staying out of the account was an option. In fact, if the defendant had left the account at this point never to return, he would have avoided further violations of law. The defendant's decision to return was based on his self-described determination to find something "incriminating" in the account.

(iii) Third Decision Point: Using A Proxy

In deciding to return to the account using the password he created, the defendant makes a third decision to use a proxy to provide some concealment of his activity. *See* Gov't Exhs. 521 (12:24:03 a.m. b tunnel.com). During the remaining period in which he alone controlled the account, he would repeatedly log into different proxy channels (b tunnel, c tunnel, d tunnel). His decision to use the proxy was not made once but several times during the period of exclusive control over the account and afterwards. *See, e.g.,* Gov't Exhs. 525 (12:48:41 a.m. using c tunnel), 532 (1:25:11 a.m. using c tunnel), 539 (1:54:14 a.m. using d tunnel), 543 (2:43:12 a.m.

151, 519; *see also* Gov't Exhs. 1, 559, 560 (describing how security questions were answered).

[2] The defendant exercised exclusive control and access over the account for nearly one hour and forty minutes (from about 12:22 a.m. EDT to 2:01 a.m. EDT on September 16, 2008).

using ctunnel).

(iv) Fourth Decision Point: Reading, Copying and Saving Images and Content

Rather than the idle curiosity of a mere trespasser, the defendant decides to read, copy and save content and images from the Governor's account onto his laptop. Images are saved on various places on his desktop and other folders on his laptop. *See, e.g.*, Gov't Exhs. 522-24, 529, 531, 533, 534, 535, 607, 619 (hard drive diagram of saved locations).

The reading of personal and confidential matters was a related decision point. As the defendant noted, his goal was to find something "incriminating." In reading the contents of the account, to his disappointment, he found nothing incriminating.

(v) Fifth Decision Point: Contemporaneously Telling Others About The Hack

Fifth, the defendant decides that it is important to let others on the Internet know that he was presently in the Governor's Yahoo! account. This step will significantly magnify the consequences of his initial actions. The defendant selects the forum, a popular Internet image board known as 4Chan.com.

During a series of posts, he describes the contents of the account and then posts screen shots of the inbox, email and contact information for others, and images. For example, the defendant makes a screen shot of the contents of the account and labels it "for great justice" before posting the screen shot onto the 4Chan site. *See* Gov't Exh. 527. This screen shot also includes the telephone number of Bristol Palin, who had shared a private family moment of the Governor's youngest son eating food for the first time, as explained at trial. After this screen shot is posted, others on the 4Chan site report calling the telephone number, during the period in

which the defendant has exclusive access to the account.

(vi) Sixth Decision Point: Emailing "i am god" Message

Sixth, while he was in the account, the defendant decides to send an email message, "i am god," from the account. This decision demonstrates his control over the account; even the account holder cannot send a message since he changed the account password.

The defendant would later refer to this message with others as proof that he was in the account. For example, at about 1:41:48 am, he posts a message to 4Chan stating, "OP here; i sent that email to confirm ... says I AM GOD." *See, e.g.*, Gov't Exhs. 527, 535, 610. About two hours later, the defendant tells his friend Ben Reed, "apparently they think im god." Gov't Exhs. 547, 548 (Facebook.com chat messages from David Kernell to Ben Reed on September 16, 2008 during 3:31:37 – 3:33:12 a.m. EDT).

(vii) Seventh Decision Point: Disregarding FBI Warnings

Seventh, during the period of the defendant's exclusive control and access, other 4Chan posters warn the defendant that the FBI has been contacted and may find him:

- 01:42:06 Lol. I just reported this to the **FBI**….
- 01:46:23 hurry before the **fbi** breaks in your house
- 01:51:11 forward all the emails to someone before the **fbi** puts you in jail please

Gov't Exh. 527 (emphasis added); *see also* Gov't Exh. 617.

How does the defendant respond to these warnings that his conduct has violated the law and that the FBI has already received a report about the crime? At one point the defendant acknowledges the FBI warnings, noting at 1:53:49 a.m. (before he decides to share the password), "im somewhat afrrid of the FBI; so ill probably go live with my uncle and auntie in

belair till this all blows over [sic]." Gov't Exh. 527. This is before his next decision to share the password.

(viii) Eighth Decision Point: Enabling Further Intrusions

Eighth, after the defendant describes on the 4Chan site his fear about the FBI, the defendant decides to access the account through a proxy one more time, this time through d tunnel. The proxy will provide some concealment about his next decision: share the password with others on the popular 4Chan site, enabling further intrusions into the account.

The defendant participates in the discussion on the 4Chan sites which shows he is fully aware of the damaging consequences. The defendant notes the potentially "ruinous" impact from further disclosure of the contents that he has already reviewed:

- 01:53:49 OP here; this is all personal stuff; ive read though it all and havent found anything inriminating; **im not going to ruin her life** and post pictures of her family; this is /b/ you know; im somewhat afrrid of the FBI; so ill probably go live with my uncle and auntie in belair till this all blows over

Gov't Exh. 527 (emphasis added). Within a few minutes, others respond:

- 01:57:21 c'mon op; you've gone this far; just post a pic- **it wont ruin her life**...
- 01:57:25 At least **give someone else the password and let *them* ruin her life**.

Gov't Exh. 527 (emphasis added).

How does the defendant respond to these suggestions? As another key decision point, the defendant, who is the only person with access (or the key) to the account, decides to provide anyone reading the 4Chan board with access. Apparently, he is comfortable letting others take steps that might "ruin her life":

- 2:01:02 "ok annon; its up to you; rapidshit this shit ok? i dont know how to do it; **ill leave it up to you**, EMAIL: gov.palin@yahoo.com PASS: popcorn"

Gov't Exhs. 527, 540 (emphasis added). In other words, while at this point the defendant has decided against posting further information from the account, in part because he does not know how to use the file-sharing service, he has no reluctance in enabling others to do so. All they need is the password, which he readily provides.

The impact is immediate. Within minutes of sharing the password, he enabled numerous individuals in the United States, New Zealand, and Canada to intrude into the account. *See* Gov't Exh. 98, 162. The trial evidence showed that others rummaged through the account and obtained images and the contents of the account. Of course, none of this would have been possible without the password that the defendant reset and shared.

(ix) Ninth Decision Point: Bragging About "Hacking" Activities

After sharing the password, the defendant then tried multiple times to log into the Governor's account but is unable to access it again. *See* Gov't Exhs. 541, 542, 543. What is his next step? The defendant's decides to brag to his friends that he had "hacked" into the Governor's Yahoo! account. Less than an hour after sharing the password, the defendant tells his friend Ben Reed in Facebook chat:

- "i hacked sarah palin's yahoo email acct"
- "im not kidding" ...
- "im somewhat afraid tho"
- "of the fbi"
- "i was behind a proxy but still"

Gov't Exhs. 123, 545, 603 (Facebook.com chat messages from David Kernell to Ben Reed on September 16, 2008 during 2:54:06 – 3:31:37 a.m. EDT). In Facebook chat with Riley Long

later the same day, he tells her about compromising the account, including some of the particulars:

- "i then posted it to this messageboard called 4chan with screenshots"
- "i kind of did something shady, but amazing last night"

Gov't Exh. 124, 552, 553 (Facebook.com chat messages from David Kernell to Riley Long on September 16, 2008 during 5:04:54 – 5:04:56 p.m. EDT).

(x) Tenth Decision Point: "Tell[ing] The Story" On 4Chan

On the next day, September 17, 2008, after the defendant has already told some of his closest friends that he "hacked" into Governor Palin's Yahoo! email account and found nothing "incriminating," what are his next steps? By chance, at this point, does the defendant recognize the wrongfulness of his conduct?

He decides to recount his hacking activity to a broader audience on the popular 4Chan site, the forum he originally selected to post the content and images from the account. In his words:

> Hello, /b/ as many of you might already know, last night sarah palin's yahoo was 'hacked' and caps were posted on /b/, i am the lurker who did it, and i would like to tell the story....

Gov't Exhs. 1, 559, 560. The defendant also explains his continuing concern about the FBI investigating his activities and steps to destroy evidence.

(xi) Eleventh Decision Point: Destroying Records

The defendant's concern about law enforcement heighten. As noted, he had already been warned multiple times that the matter had already been referred to the FBI before he decided to share the password. *See* Gov't Exh. 527. After sharing the password, he even told his friend Ben

Reed that he was "somewhat" concerned about the FBI. *See* Gov't Exh. 122. In a Facebook message, his friend Riley Long also refers to the FBI. *See* Gov't Exh. 120. The defendant receives more warnings about the FBI, including:

- Sept. 17, 2008 1:11:20 p.m. You know Moot has to cooperate with the FBI and you just admitted to a felony. Your seven proxies won't save you. Me calling the FBI right now to harass you for this hoax is far more epic than this sad hoax.

Gov't Exh. 617.

On September 17, 2008, the defendant receives a warning that someone has discovered his identity:

- Sept. 17, 2008 9:58 p.m. Hi, I found your email address when googling about the /b/ email story ... and when I googled "rubico10", I found a blog where someone posted a link to your blog (apparently from 2003) Just thought you should know that you should take it down, because it seems to reveal your real name Best of luck

Gov't Exh. 563. After receiving this message, the defendant takes steps to modify his "rubico10" profile.

The defendant begins to research the consequences of his actions. His Google searches include: "legalities email," "legalities yahoo email," Stored Communications Act or SCA," "sopena [sic] ip addresses." *See, e.g.*, Gov't Exh. 152, 519, 576-596, 622, 623.

What choices does he face at this juncture? Can he take steps to mitigate the harm his actions have caused up to this point? Is contacting law enforcement an option on his own (based on other reports that law enforcement has already been contacted)?

After learning more about how serious his actions were, and against the backdrop of the

warning of the FBI being contacted, the defendant selects several discrete steps to destroy evidence. As forensic testimony at trial established, these steps included:

- Deleting various folders and images he obtained from the Governor's Yahoo! Account which were saved in different locations on his laptop (including the D:\b folder; Palin folder; My Pictures folder; and desktop)
- Clearing his Internet Explorer web browser cache (deleting Internet activity during deleting September 13 to September 18, 2008 activity)
- Uninstalling his Mozilla Firefox web browser uninstaller program
- Deleting his temporary internet files
- Running the Disk Defragmenter program

See, e.g., Gov't Exhs. 569, 572, 599. As a result of these actions, when the defendant's laptop is seized pursuant to a search warrant, a substantial amount of data was unrecoverable from the hard drive. As shown at trial, in many instances, only partial images remained from the Governor's account. Some relevant information was found in freespace (deleted data on the hard drive subject to being overwritten by other data), but the information was incomplete. There were significant gaps in the evidence on the laptop based on the records that were deleted and unrecoverable. Significantly, the defendant was successful in removing a substantial amount of data concerning recent Internet activities on the laptop, which is how the offense was committed.

(xii) Eleven Key Decision Points

As the evidence at trial demonstration, there were at least eleven key decision points the defendant confronted. Each point provided a chance to mitigate the harm that had been caused. Instead of mitigating the consequences of his harm, the defendant repeatedly took the path which exacerbated the circumstances.

2. Victim Impact and Intended Impact

In assessing the nature and circumstances, it is also useful to consider the consequences of the defendant's conduct on the victims and the intended impact of his actions.

The defendant intended that his conduct would be highly disruptive from the inception. In his own words, his plan was to find "incriminating information" in the account which could be used to "derail" a national campaign. Gov't Exhs. 1, 559, 560.[3] Ultimately, the defendant was disappointed and concluded "there was nothing."[4]

Notwithstanding his objectives, the consequences of the defendant's conduct on the victims was almost immediate and significant. Governor Palin already described at trial the

[3] During the period in which the defendant had exclusive control over the account, the defendant provides updates on what he is doing and posts images and content from the account. Some 4Chan poster posters noted the potential consequences on upcoming national campaign:

- 01:36:20 if this is real its the greatest moment in /b/ history.
- 01:41:52 OP I believe you have the power to bring down the McCain campiagn please use your power wisely
- 01:43:04 hey OP is Jon McClain's personal email in there? get that and hack it as well
- 01:46:16 If this is real; and you upload this; you will change fucking history

Gov't Exh. 527.

[4] *See also* Gov't Exh. 546, 547 (noting "nothing incrimiating:(" "nothing incrimiating" [sic]) (sad face expression in original) (Facebook.com chat messages from David Kernell to Ben Reed on September 16, 2008 during 2:54:06 - 3:31:37 a.m. EDT); 552, 553 (noting "i looked though it "and sadly, nothing incriminating") (Facebook.com chat messages from David Kernell to Riley Long on September 16, 2008 during 5:04:54 – 5:04:56 p.m. EDT); 553, 554 ("haha i wanted to see if she was corupt"; "i didnt find aything") (Facebook.com chat messages from David Kernell to Riley Long on September 16, 2008 during 5:04:56 – 5:05:37 p.m. EDT); 557, 558 (noting "if there was something incriminating in there"; "oh my god the possibilities"; "but sadly there wasnt" [sic]) (Facebook.com chat messages from David Kernell to Riley Long on September 16, 2008 during 5:23:06 – 5:23:09 p.m. EDT).

impact the conduct had on a personal level but also as Governor and candidate for Vice President, which will not be repeated here.

The impact clearly went beyond the Governor. As part of the relevant conduct, the Court should consider all the persons that were impacted as a result of the defendant's decisions and actions. There were numerous victims in this case Shortly after the defendant posted information and images from the account, the Governor's contacts began receiving numerous unsolicited messages, many of them crude and vulgar. As a direct result of the defendant's actions, the contacts in the account received unwanted messages, including some emails repeatedly using the "n" word and "Sucks Moose Cock !!!!!," among many others. *See* Gov't Exhs. 30, 32. While the defendant did not send these messages, none of them could have been sent without the defendant disclosing the contact information from the account.

As noted at trial, the defendant also made the screen shot of the inbox of the account, which included Bristol Palin's telephone number, at 1:20:24 a.m. as the second listed e-mail entry. *See, e.g.*, Gov't Exh. 11. This message included a photograph of a personal, private moment involving the Governor's youngest son. The defendant posted the screen shot of the emails on 4Chan at 1:21:43 a.m., adding the caption "for great justice." Shortly after words, the 4Chan posters begin discussing and calling the telephone number:

- 01:30:57 someone call that number in the screencap and confirm; gogogo
- 01:34:04 Called the number a young girl picked up and i didn't really want to talk so i just said wrong number. This shit is a little dangerous for mw to get into /b/
- 01:35:34 THIS IS THE REAL SHIT I HAVE CONFIRMED NUMBER AND ALL THE CONTACTS IVY FRYE IS AK STATE SEN< EPIC EPIC EPIC

Gov't Exh. 527. As Bristol Palin, the Governor's daughter, testified at trial, she received numerous unwanted telephone calls and text messages as her phone number was displayed in the

screen shot the defendant took of the account and posted on 4Chan. *See also* Gov't Exhs. 87, 88 (summary of unwanted calls and texts). As established at trial, before the defendant decided to share the password, he was aware that other individuals were being impacted by his conduct.

b. History and Characteristics of the Defendant

(1) *Criminal History*

Under Section 3553(a)(1), the defendant does not have any prior criminal conviction. However, the defendant had a prior incident in school involving the use of a password. This was not the first time that he was engaged in unauthorized access conduct. In 2001, when the defendant attended Eastern Hills Middle School in Killeen, Texas, he spent time working on computers and playing computer games. During one incident, he and another student guessed the password of a school server and gained access to the school server, which included lesson plans. A teacher discovered that a computer terminal was connected to the server and found that the defendant had logged on. The defendant was determined to be responsible for this unauthorized access.

(2) *Personal History And Characteristics*

Under Section 3553(a)(1), the personal history and characteristics of the defendant reveal a person who has a clear disregard for the law.

Before the Court is an individual who in the face of multiple "red flag" warnings about a federal investigation and possible violations of law proceeds with his actions. Instead of stopping or mitigating his conduct, the defendant decides he should continue rummaging through and sharing the contents of the account. For example, during the period from 1:42:06 a.m., when the first information about an FBI report was made, and 1:53:49 a.m., when he acknowledges his

fear about the FBI, the defendant continued to locate and save images from the Yahoo! account.

Significantly, once the defendant researches and realizes the seriousness of his conduct, his next step is to destroy records of his involvement. This conduct shows a complete disregard for the integrity of the law enforcement and judicial process.

The defendant was fully aware of the "ruinous" impact of his consequences which he and others discussed on the 4Chan site. Knowing the consequences of his conduct, he willingly proceeded to share the password he created which permitted others around the world to intrude into the account. About fifteen hours after sharing the password, at one point the defendant tells his friend Riley Long, "i kind of did something shady, but amazing last night." Gov't Exh. 552, 553 (Facebook.com chat messages from David Kernell to Riley Long on September 16, 2008 during 5:04:54 – 5:04:56 p.m. EDT). There is no meaningful hint of any understanding of the wrongfulness of his action which he considered to be "amazing." It was only after he learned he could be discovered that the decided it was important to destroy records.

Further insight into the "true" character of the defendant is shown by his response after he shared the password. Another person, who the defendant referred to as the "white knight," tried to alert Ivy Frye that the account had been "hacked," as she testified at trial. *See* Gov't Exhs 24, 25, 26 (messages to I've Frye warning that the account had been "hacked"). In the defendant's view, his "hacking" conduct was justified but the actions of the white knight were not. As the defendant explained in his September 17th Rubico post:

> Then the white knight fucker came along, and did it in for everyone, I trusted /b/ with that email password, I had gotten done what I could do well, then passed the torch , all to be let down by the douchebaggery, good job /b/, this is why we cant have nice things

Gov't Exhs. 1, 559, 560. The defendant's misplaced notions of right and wrong are captured in

this statement.

It is therefore not surprising that he disregarded multiple warnings about a federal investigation. In his view, his violations of law were justified by his motive to derail a national campaign. In other words, in his view, the ends justified the means, notwithstanding clear warnings along the way. When there is a risk of discovery, his reaction is to destroy records.

2. Need To Reflect The Seriousness Of The Offense

Under Section 3553(a)(2)(A), the requested prison term is necessary to reflect the seriousness of the defendant's conduct, promote respect for the law, and provide just punishment for the offense.

As noted, the conduct was intended by the defendant to be serious. His goal was to influence a national election. The only reason his conduct was not successful was that he found "nothing incriminating" in the account, much to his disappointment. He persisted on his course despite being aware of the potentially "ruinous" consequences of his conduct and in the face of multiple law enforcement warnings.

Perhaps most significant are the steps the defendant took to destroy records of his activities. Once he realized the full risk of a federal investigation, he destroyed records concerning his activities. This conduct goes to the integrity of the process and undermines the truth seeking function of the investigation and judicial system.

In particular, Section 1519 was enacted by Congress to address the circumstance where an individual destroys evidence in anticipation of a federal investigation. Congress intended to protect the integrity of federal investigations and the administration of justice. As noted in the Senate Report:

> Section 1519 is meant to apply broadly to any acts to destroy or fabricate physical evidence so long as they are done with the intent to obstruct, impede or influence the investigation or proper administration of any matter, and such matter is within the jurisdiction of an agency of the United States, or such acts done either in relation to or in contemplation of such a matter or investigation…. It also extends to acts done in contemplation of such federal matters, so that the timing of the act in relation to the beginning of the matter or investigation is also not a bar to prosecution. **The intent of the provision is simple; people should not be destroying, altering, or falsifying documents to obstruct any government function**.

Sen. Rep. No. 146, 107th Cong., 2d Sess. 14-15 (2002) (emphasis added). The legislative history further notes:

> We recognize that section 1519 overlaps with a number of existing obstruction of justice statutes, but we also believe it captures a small category of criminal acts which are not currently covered under existing laws — for example, **acts of destruction committed by an individual acting alone and with the intent to obstruct a future criminal investigation**.

Sen. Rep. No. 146, 107th Cong., 2d Sess. 27 (2002) (emphasis added).

In this case, the defendant's conduct can be seen as part of an ongoing series of actions he embarked on. Initially, he tries to influence a national election. He selects a proxy to provide some concealment of his intended actions. He selects an Internet forum that permits anonymous posting. Even when told repeatedly that his conduct has already been reported to law enforcement, he persists. Initially he believes he is beyond the reach of law enforcement and can avoid detection. When he suddenly realizes that he can be found, he then tries to influence the administration of justice.

3. Deterrence Of Criminal Conduct

By imposing the recommended prison sentence, under Section 3553(a)(2)(B), the Court has the opportunity to have a meaningful specific and general deterrent effect. The defendant will be specifically deterred from committing more crimes. It is worth noting that the defendant, during the pendency of this case, did not seem to view his conduct as serious or criminal. His view seems to be that his conduct was merely an immature college prank.

Moreover, the prison sentence will deter others from committing similar offenses. Anyone who seeks to destroy records as part of an effort to influence the administration of justice deserves a significant sentence. Further, anyone else who may contemplate "hacking" into the account of a public official with the hopes of "derailing" a campaign and then destroying evidence of this conduct in anticipation of a federal investigation should know that the conduct is subject to a significant prison term.

4. Need To Protect The Public

Under Section 3553(a)(2)(C), the public needs to be protected from individuals who intentionally set out to commit serious offenses, which are aggravated by the destruction of evidence.

5. Need To Provide The Defendant With Education

Any need to provide the defendant with education and vocational skills under Section 3553(a)(2)(D), while important in many contexts, is subordinate in this case to the important considerations of deterrence, protection of the public and the need for the sentence to reflect the seriousness of the offense. *See United States v. Wilson*, 350 F. Supp. 2d 910, 921-22 (D. Utah 2005) (noting that legislative history of Sentencing Reform Act demonstrates that Congress intended to place rehabilitation as a secondary consideration where serious crimes were

involved). The defendant will have access to many programs in the prison system to which he can avail himself. Neither the presence nor absence of any further educational programs should weigh heavily in this Court's sentencing determination, in this case.

6. Kinds of Sentences and the Sentencing Range

As noted above, the applicable Sentencing Guideline range results in a term of 15 to 21 months. In this case, the government requests a mid-range sentence of 18 months in prison.

7. Any Pertinent Policy Statements

The prison term is consistent with Sentencing Guideline policy statements, which recognize certain aggravating conduct, as committed in this case, is subject to an upward departure.

First, based on the evidence at trial, it is clear that the defendant was motivated by Governor Palin's official status as Governor of Alaska and the Republican nominee for Vice President. Every four years, there are only two persons selected as a candidate for Vice President of the United States. The defendant selected one of them during the 2008 national election.

> As a pertinent policy statement, U.S.S.G. § 3A1.2(a), comment. (n.5) expressly notes: If the official victim is an exceptionally high-level official, such as the President or the Vice President of the United States, an upward departure may be warranted due to the potential disruption of the governmental function.

In this case, with only weeks before the national election, the defendant targeted the account of one of the two national Vice Presidential candidates. His stated purpose was to find "incriminating information" which he could use to "derail the campaign." One of the governmental functions the defendant sought to disrupt was the national election, which embodies one of the cornerstones of our democracy.

Second, after reviewing the contents of the account, the defendant decided to publicly disclose personal information. Under U.S.S.G. § 2B1.1(a), comment. (n.1), "personal information" includes:

> sensitive or private information involving an identifiable individual (including such information in the possession of a third party), including ... (C) diaries; (D) private correspondence, including e-mail; ... (F) photographs of a sensitive or private nature; or (G) similar information.

An upward departure consideration is warranted where, as here: "A primary objective of the offense was an aggravating, non-monetary objective." Under U.S.S.G. § 2B1.1(a), comment. (n.19(a)(i)). As noted, here the primary motivating factor was to find "incrimination information" to "derail" a national campaign.

Third, an upward departure may be appropriate in cases involving "a substantial invasion of a privacy interest." U.S.S.G. § 2B1.1(a), comment. (n.19(a)(ii)).

Finally, under U.S.S.G. § 5K2.9, as an encouraged factor, a departure may be warranted:

> If the defendant committed the offense in order to facilitate or conceal the commission of another offense, the court may increase the sentence above the guideline range to reflect the actual seriousness of the defendant's conduct.

While the government is not requesting an upward departure from the applicable Sentencing Guideline factors, noted above, it does believe that these policy statements firmly support the requested term of imprisonment. Additionally, these policy statements may offset any downward departure bases offered by the defense.

8. Need to Avoid Unwarranted Disparity In Sentences

On "the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct," under Section 3553(a)(6), this case stands alone in many respects.

The recommended sentence is actually below many other obstruction of justice convictions, based on the most recently available information from the U.S. Sentencing Guidelines Commission. *See* Attachment. Under the "Administration of Justice Offenses," where Section 1519 offenses are grouped, when a prison term is imposed, the mean term of imprisonment for criminal history category one offenders is 20 months.

In many respects, this case stands alone. There are few destruction of record cases which involved an effort to remove evidence involving conduct which was intended to influence a national election. The defendant target a national official based on her recent selection as Republican nominee for Vice President. Instead of merely trespassing into the account and leaving (as he did during the first two minutes of exclusive access), he returned, copied images and other information, posted content from the account on the Internet, provided others with the password he created to the account. He did after others had warned him about the incident being reported to the FBI. In anticipation of the federal investigation, he destroyed records about his involvement.

9. Need To Provide Restitution To Any Victims Of The Offense

The need to provide restitution is not an issue in this case. 18 U.S.C. § 3553(a)(7).

VI. Conclusion And Recommended Sentence

As discussed above, the applicable Sentencing Guideline and Section 3553(a) sentencing factors support the requested imprisonment in this case. Based on the seriousness of the offense, including the steps taken to destroy records, the government urges the Court to impose the requested prison term in this case. Based on the foregoing, and consistent with the evidence at trial, the government respectfully requests that the Court sentence the defendant to a mid-range term of eighteen months in prison.

Respectfully submitted this 27th day of October, 2010.

WILLIAM C. KILLIAN
United States Attorney

S/ D. Gregory Weddle
S/ Mark L. Krotoski
S/ Josh Goldfoot

_____

D. Gregory Weddle
Mark L. Krotoski
Assistant U.S. Attorney
800 Market Street, Suite 211
Knoxville, TN 37902
865-225-1710

Josh Goldfoot
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice
1301 New York Ave. NW
Washington, DC 20005

CERTIFICATE OF SERVICE

I hereby certify that on October 27, 2010, a copy of the foregoing

GOVERNMENT'S SENTENCING MEMORANDUM

was filed electronically. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic filing receipt. All other parties will be served by regular U.S. mail. Parties may access this filing through the Court's electronic filing system.

S/ D. Gregory Weddle

_____

D. Gregory Weddle
Assistant U.S. Attorney
800 Market Street, Suite 211
Knoxville, TN 37902
865-225-1710