MICHAEL J. PROUT
Assistant Director for Judicial Security
United States Marshals Service

Written Statement Presented to the
United States Sentencing Commission
Public Hearing on the Court Security Improvement Act of 2007

March 17, 2009

On behalf of the United States Marshals Service (USMS), we submit the following comments concerning two criminal provisions of the Court Security Act of 2007, 18 U.S.C. § 115 and 18 U.S.C. § 119, particularly with respect to violations that occur through the use of the Internet.

18 USC §115 prohibits threatening a Federal official to influence, impede, or retaliate against a Federal official who is performing official duties. This statute specifically mentions the Federal judiciary and is of particular interest to the USMS. The Court Security Act of 2007 increased the statutory maximum penalty for this crime to ten years, except that imprisonment for a threatened assault cannot exceed six years.

18 USC § 119 is a new law that makes it illegal to intentionally release personal restricted information (*i.e.* Social Security number or a home address) with the intent to threaten, intimidate, or incite the commission of a crime of violence to a covered person, such as a judge, Assistant United States Attorney, federal law enforcement officer, or a member of their family. Violations of this section are punishable by imprisonment of up to five years.

For the purpose of this report, we defined "through the use of the Internet" as writings or other information posted on an Internet website or blog. We consider these threats to be more serious than written communications sent solely via email. In terms of impact to the victim, and the potential to incite others, we do not consider a communication sent via email to be much different than communication sent via regular mail. The exception to this rule is if the emailed communication, by virtue of being sent to a private or unlisted email account, shows evidence of exceptional research on the part of the sender, increasing the likelihood that the sender's next step is to personally approach the protectee.

On the other hand, we view inappropriate communications and threats made via Internet postings and blogs very differently than other delivery methods. Unlike a letter or an email, comments posted on an Internet website have the potential to be viewed by a countless number of persons. Internet postings that are hyper-critical and contain restricted personal information of the protectee, such as a home address or Social Security number, can create a large number of potential threateners virtually unknown to the USMS. Such a scenario can be extremely difficult to accurately assess and can lead

to the expenditure of an extraordinary amount of resources to ensure the safety of our protectees.

Internet threats should also be differentiated from other types of "public forum" events, such as radio, television, or a speech made in a public setting. While these forums can also reach a large, unknown audience, their impact is more limited as they generally reach only the audience that happens to be listening or viewing them at that particular moment, and they are done in a public forum which can easily become known to law enforcement. The audience to an Internet threat can be multiplied exponentially, and the blog or website may be completely unknown to law enforcement.

At this point, a brief explanation of our definitions for an inappropriate communication and a threat is warranted:

- A **threat** is defined as an inappropriate interest, circumstance, or event that causes, or could potentially cause, damage to a target whether it is a person, location, or specific event. A threat can be any action, whether explicit or implied, of intent to assault, resist, impede, intimidate, or interfere with any member of the judiciary, or other protectee. A threat may be communicated in writing, verbally or through a third party.

- An **inappropriate communication** is any communication in writing, by telephone, verbally, through an informant, or by some suspicious activity that threatens, harasses, shows an unusual direction of interest, or makes unsettling overtures of an improper nature directed to a protectee.

- A **threat** is always an inappropriate communication, but an **inappropriate communication** is not always a threat.

Most Internet threateners, when confronted or challenged on their statement, will claim they are only exercising their First Amendment right to free speech. And in many cases, an examination of their speech could lead us to concur. To guard against violating a person's First Amendment right to free speech, the USMS requires the occurrence of a "triggering event" before a protective investigation is initiated. In the area of threat management, a "triggering event" is the receipt of an inappropriate communication, or a reasonable indication that a possible threat exists. However, one of the issues that make Internet threats so insidious is that *others* who hear or read this "free speech" may interpret it differently; they may interpret it as a threat of violence, or as a call to violence, and be influenced to act out violently. If the threat on the Internet is also accompanied by restricted personal information, it can assist in facilitating the act of violence by locating the protectee.

Internet Threats by the Numbers

In the last five years, inappropriate communications (ICs) to USMS protectees has increased 89%. Threats received via the Internet have followed this trend. The following statistics illustrate this trend:

FY 03

674 Total ICs received (no further breakdown available)

FY 04

873 Total ICs received (no further breakdown available)

FY 05

943 Total ICs received (no further breakdown available)

FY06

1,111 -	Total ICs received	
651 -	ICs received via written method of delivery	
12 -	*ICs received via Internet posting or blog*	**(1.0% of total ICs)**

FY07

1,145 -	Total ICs received	
632 -	ICs received via written method of delivery	
13 -	*ICs received via Internet posting or blog*	**(1.1% of total ICs)**

FY08

1,278 -	Total ICs received	
724 -	ICs received via written method of delivery	
15 -	*ICs received via Internet posting or blog*	**(1.2% of total ICs)**

FY09 (to date)

478 -	Total ICs received	
265 -	ICs received via written method of delivery	
8 -	*ICs received via Internet posting or blog*	**(1.7% of total ICs)**

Recipients of Internet Threats

While our database is capable of determining separate categories of recipients, it does not differentiate written threats received via regular mail and threats received via the Internet. These numbers were determined through a hand search of the last 3 ½ years of data.

In the vast majority of these Internet cases, the threat or inappropriate communication was directed at a single, case-specific victim, usually the presiding judge in a particular case. In rare cases, the threats made reference to more than one judge, or to a prosecutor or case agent. Internet cases do not necessarily create volumes of victims; they do, however, create volumes of potential threateners.

Additionally, our numbers only catch the number of Internet threats and inappropriate communications that were reported to us. It is impossible to determine how many threats and ICs occurred everywhere on the Internet, just as it is impossible to determine who has seen these threats.

Senders of Internet Threats: Individuals v. Groups

In most cases, Internet threats are posted by individuals. However, these individuals are frequently part of a group, or at least communicating through the Internet with other like-minded individuals.

We are experienced in managing and mitigating threats posed by known individuals and groups. Threats from the Internet can create a large pool of "unknown threateners," difficult to identify and more difficult to mitigate. As such, there is a much greater chance that an Internet threat will result in protective measures, with a greater expenditure of resources. But because of the size and scope of the Internet, there is also a great chance that many Internet threats, while potentially widely seen by others, will never come to our attention, and hence never be investigated or mitigated.

Additionally, today's terrorist groups, both domestic and international, use the Internet as a tool to communicate and incite others to violence. For example, leaderless cells and the lone wolf convey ideology via the Internet. White supremacists, animal rights extremists, and eco-terrorists use the Internet to communicate, recruit, and intimidate.

The following are a few examples of different types of Internet-related threats and inappropriate communications we have encountered. Some of the examples make reference to groups, some organized and well-defined, others simply like-minded sympathizers. For classification purposes, the USMS views all of these as originating from an individual, despite their potential to influence and incite others. A threat with a known group affiliation may assist us in defining its range of influence or potential for a particular type of

reaction, but is not necessarily more or less sinister than a threat posted by an individual with no known group affiliation.

Judge on the Southwest Border

In February 2009, a Federal judge heard a civil case where illegal aliens sued a rancher, a U.S. citizen, for violating their civil rights by detaining them as they illegally entered the United States through his ranch. The judge rejected a motion to dismiss the case and the case went to trial. One individual posted the judge's home address on a blog. Many others responded with comments on the blog that were threatening, stating the judge should be shot, hung and other violent acts. The judge also received hundreds of phone calls at the courthouse, many that were threatening and inappropriate. As a result a protective detail was established.

Radio Talk Show Host

In June 2008, a white supremacist radio talk show host released the home addresses (current and past), telephone numbers and work address of two Federal judges on his radio broadcast, and on his show's website, because he did not like decisions they made pertaining to immigration. He announced that both judges were traitors to the United States. He called for citizens to visit the judges at home, away from the protection of the USMS. He suggested face-to-face confrontation as a method for airing discontent with the rulings. He said that he could picture himself punching out these judges, kicking them in the ribcage and in the head, and then challenging them on their decisions while they lay on the ground. He remarked that "he would have a really good time beating the shit out of a federal judge (sic)" and suggested that his listeners would enjoy this activity as well. His intention was to incite others to attack these judges. This activity resulted in establishing a protective detail.

Ed Brown and the United States Constitution Rangers

Ed and Elaine Brown were members of the United States Constitution Rangers (USCR), an anti-government, anti-tax organization, originally established in Arizona in 1977. In January 2007, the Browns were convicted of tax evasion and remained in their house in New Hampshire refusing to come out. The Browns themselves made no threats to any judicial or law enforcement official. However, one of their supporters posted a letter on the Internet stating the judge and U.S. Attorney and various other officials should be hanged for treason for their actions against the Browns. This initiated a long Internet campaign of threats and ICs directed at USMS protectees from the Browns' supporters and other anti-government and anti-tax groups. This activity resulted in protective details on several judges and prosecutors.

Conclusion

The USMS is concerned about the use of the Internet to threaten and intimidate its protectees and appreciates the opportunity to address the U.S. Sentencing Commission. The consideration to increase penalties is a valuable tool for the challenge the USMS faces to protect the judiciary.