

USMS had taken to improve judicial security and to enhance its capability to respond to judicial security incidents.<sup>44</sup>

The OIG found that USMS efforts to improve its capabilities to assess reported threats and identify potential threats languished from the issuance of the March 2004 report to early 2007. We found that threat assessments took longer to complete, resulting in a backlog of 1,190 "pending" threat assessments as of October 1, 2006. Further, the USMS did not implement an effective program to develop protective intelligence that identified potential threats against the judiciary.

To improve the USMS's capacity to protect the federal judiciary, the OIG made six new recommendations. Since September 2007, the USMS has reported to the OIG the steps it has taken to implement them. For example, the USMS developed plans to improve its threat assessment process and for implementing a protective intelligence function to identify potential threats, including objectives, tasks, milestones, and resources. The USMS created a *Guide for Office of Protective Intelligence Personnel to Coordinate Protective Investigations*, which describes a comprehensive strategy for handling protective investigations and is in the process of modifying its inappropriate communication Threat Module of the Justice Detainee Information System (JDIS) to produce more user-friendly reports. Also, the USMS is finalizing policies for Technical Operations Group support concerning protective operations and investigations for Judicial Security Rapid Deployment Teams. The OIG has closed four of the six recommendations.

---

<sup>44</sup> Department of Justice, Office of the Inspector General, *Review of the United States Marshals Service Judicial Security Process*, Evaluation and Inspections Report I-2007-0104, September 2007.

**APPENDIX II: METHODOLOGY OF THE OIG REVIEW**

---

The methodology used in this review included interviews with USMS, EOUSA, and FBI personnel, as well as site visits to four federal judicial districts where we interviewed federal judges, USMS personnel, AUSAs, and other USAO personnel. In addition, we conducted a survey of a stratified random sample of AUSAs and performed document reviews and database analyses.

Interviews at USMS Headquarters and EOUSA

To determine the role and responsibilities of the USMS and the role of EOUSA in the protection of federal judges, U.S. Attorneys, and AUSAs, we interviewed 10 individuals: 4 from USMS headquarters at the Judicial Security Division and 6 from EOUSA. At USMS headquarters, we interviewed the Chiefs of the Office of Protective Operations, the Office of Protective Investigations, the Office of Court Security, and the Threat Management Center. At EOUSA, we interviewed the Director of EOUSA, the Chief of the Security Programs Staff, a Threat Management Specialist, a Physical Security Specialist, a Program Assistant for the Mission Assurance Team, and a Program Assistant for Physical Security.

Site Visits

We conducted site visits at four judicial districts. We chose the districts based on the number and severity of threats received by federal judges, U.S. Attorneys, and AUSAs in the districts, the number of prosecutors in the districts, and geographic location.

During these site visits, we conducted interviews and reviewed documents at four USAOs and four USMS district offices. At each USAO, we interviewed the U.S. Attorney, the Regional Security Specialist, the District Office Security Manager, and four AUSAs. At each USMS district office, we interviewed the U.S. Marshal, the Judicial Security Inspector, and at least one District Threat Investigator. We also interviewed at least two federal judges in each district to determine their experiences with protective measures provided after the judge received a threat. At three of the sites, we interviewed the judge who served as the Chair of the Court Security Committee for that district.

At each site, we also interviewed an FBI Special Agent who performed criminal investigations of threats against federal judges and AUSAs to

determine how the FBI and USMS coordinate their simultaneous investigations. In total, we interviewed 60 individuals in the field. When we report the percentage of site visit interviewees who held a particular opinion in our findings sections, we based the percentage on the number of people who answered a specific question on that topic instead of on the total number of interviewees.

### Survey

We conducted a web-based survey of a stratified random sample of U.S. Attorneys and AUSAs to assess how they perceived the extent of the security provided to them in response to the threats they received. We also sought to determine what security measures were provided in response to threats received, as well as what security training was provided by the USMS and their respective USAOs. Using demographic data supplied by EOUSA about current AUSAs, we assigned the attorneys to different subsets and selected a random sample within each subset. The subsets were defined by three demographic factors: gender, length of service as a federal prosecutor, and the number of personnel working at the USAO.

We sent an invitation to participate in the web-based survey to the 688 U.S. Attorneys and AUSAs. We received 383 responses, a 56-percent response rate.

Some survey questions required respondents to select from pre-determined responses, while other questions allowed respondents to respond in their own words. In choosing the respondents' comments included in the body of this report, we selected those that were the most representative of the opinions expressed by the respondents.

Appendix III contains a copy of the survey and the results.

### Document and Database Review

To determine the role and responsibilities of the USMS headquarters and the district offices in the protection of federal judges, U.S. Attorneys, and AUSAs and the response to threats received by those individuals, we reviewed the USMS's mission, directives, policies, and manuals; performance measures; budget documents; federal laws; and threat data from the Threat Management Center.

To determine the number and types of threats received by federal judges, U.S. Attorneys, and AUSAs in various districts, we reviewed USM-11

Report of Investigation forms and USM-550 Preliminary Threat Report forms from the USMS Threat Management Center database.<sup>45</sup> We also used the database to assist in determining:

- the sites to visit based on the number and severity of threats per district;
- the federal judges, U.S. Attorneys, and AUSAs to interview regarding their experiences in receiving threats;
- the average time for the USMS to respond to a threat;
- the risk levels assessed to each threat by the USMS; and
- the protective measures that were provided to threatened federal judges and AUSAs in response to various threats.

To examine the role and responsibilities of EOUSA in the protection of U.S. Attorneys and AUSAs, we reviewed EOUSA's mission, policies, procedures and manuals; training materials; budgets for protective measures; Urgent Reports submitted by the USAOs when a threat was received; and the EOUSA threat database.

To determine the role of the USAOs in the protection of U.S. Attorneys and AUSAs, we reviewed office security plans; Urgent Reports generated when a threat was received by an attorney; security training materials; position descriptions for security-related positions; and budget requests pertaining to security for each of the four districts we visited.

---

<sup>45</sup> USM-11s and USM-550s contain a summary of the threat event, information on the suspect, and a report of investigation containing a synopsis of the protective investigation.

**APPENDIX III: RESULTS OF OIG SURVEY OF U.S. ATTORNEYS AND ASSISTANT U.S. ATTORNEYS**

We conducted a web-based survey of a stratified random sample of U.S. Attorneys and Assistant U.S. Attorneys (AUSA) to assess how they perceived the extent of the security provided to them in response to the threats they received. We sent invitations to participate in the web-based survey to the 688 members of the chosen sample. Three hundred eighty-three attorneys in 30 districts responded to the survey.

Note: When percentages do not add to 100, it is because of rounding.

**Background Questions**

- 1) Are you a U.S. Attorney or an AUSA?

<b>Attorney Type</b>	<b>Number</b>	<b>Percentage</b>
U.S. Attorney	8	2%
AUSA	375	98%
<b>Total</b>	<b>383</b>	<b>100%</b>

- 2) Are you male or female?

<b>Gender</b>	<b>Number</b>	<b>Percentage</b>
Female	139	36%
Male	244	64%
<b>Total</b>	<b>383</b>	<b>100%</b>

- 3) What district do you work in?

<b>District</b>	<b>Number</b>	<b>Percentage</b>

District	Number	Percentage
<b>Total</b>	<b>383</b>	<b>100%</b>

4) How many attorneys are in your district office?

Attorneys Per Office	Number	Percentage
1-29	79	21%
30-99	132	35%
100+	172	45%
<b>Total</b>	<b>383</b>	<b>100%</b>

5) Since January 1, 2006, what type of matters do you primarily handle?

Matter Type	Number	Percentage
Civil	75	20%
Criminal	308	80%
<b>Total</b>	<b>383</b>	<b>100%</b>

- 6) How many years' experience do you have as an AUSA or U.S. Attorney?  
(Include all the years you worked at any USAO as an attorney.)

<b>Years' Experience</b>	<b>Number</b>	<b>Percentage</b>
Less than 1 year	45	12%
1 to 3 years	49	13%
4 to 9 years	73	19%
10 to 14 years	83	22%
15+ years	133	35%
<b>Total</b>	<b>383</b>	<b>100%</b>

- 7) What type of case do you believe poses the greatest risk of receiving threats?

<b>Case Type</b>	<b>Number</b>	<b>Percentage</b>
Drugs	100	26%
Gangs	171	45%
Pro se (criminal defendant)	24	6%
Pro se (civil party)	33	9%
Public corruption	2	1%
Terrorism	13	3%
Tax (civil)	5	1%
Tax (criminal)	10	3%
Other	25	7%
<b>Total</b>	<b>383</b>	<b>100%</b>

Twenty-five respondents chose "Other" and provided answers in their own words. The OIG categorized information within their answers as follows:

<b>Category</b>	<b>Number of Responses</b>
All criminal cases	1
Any type of case	1
Civil rights	1
Depends on defendant	2
Firearms	3
Foreclosures/collections	1
Forfeiture	2
Fraud	2
Gangs & drugs	1

<b>Category</b>	<b>Number of Responses</b>
Irate family members	1
Judgment debtors	1
Liberty & property	1
Organized crime	3
Violent crime	1
White collar	2
Don't know	2
<b>Total</b>	<b>25</b>

N=25

N represents the number of respondents.

- 8) If you answered "Other" to the previous question, please specify whether the case was civil or criminal.

<b>Civil or Criminal Case</b>	<b>Number of Responses</b>
Criminal	19
Civil	2
Civil & criminal	1
Respondent answered forfeiture but did not classify the cases as civil or criminal	1
Respondent answered risk was not case-related but rather was dependent on the defendant's tendency toward violence and mental history	1
Respondent answered that he did not know what type of case posed the greatest risk, but then also answered criminal when asked to specify a civil or criminal case	1
<b>Total</b>	<b>25</b>

N=25

- 9) Do you know what procedures to follow in the event you, or a family member, receive a work-related threat?

<b>Yes/No</b>	<b>Number</b>	<b>Percentage</b>
Yes	308	80.4%
No	74	19.3%
No answer	1	0.3%
<b>Total</b>	<b>383</b>	<b>100%</b>



- 10) Have you, or an immediate family member, personally received a threat since January 2006 related to your employment at the USAO? (Please answer “yes” to this question only if you believe the threat was related to your employment at the USAO.)

<b>Yes/No</b>	<b>Number</b>	<b>Percentage</b>
Yes	61	16%
No	322	84%
<b>Total</b>	<b>383</b>	<b>100%</b>

- 11) If you answered “Yes” to the previous question, please specify how many threats you received since January 2006.

<b>Number of threats</b>	<b>Number of responses</b>
One threat	37
Two threats	11
Three threats	6
More than three threats	1
<b>Total</b>	<b>55</b>

N=55

Only 55 of 61 respondents who reported receiving threats in Question 10 answered this question.

One of the 55 respondents to this question reported receiving over 1,000 threats.

- 12) What types of work-related threats have you received? (Check all that apply.)

<b>Threat Type</b>	<b>Number Of Responses</b>
E-mail	3
Face-to-face	15
Letter	12
Telephone call	12
Other	29
<b>Total</b>	<b>71</b>

Respondents could select more than one response.

Twenty-nine respondents chose “Other” and provided answers in their own words. The OIG categorized information within their answers as follows:

<b>Origin of Threat</b>	<b>Number of Responses</b>
Third party (e.g., informant)	18
Person followed family member	1
Written threat	4
Discovered by investigators	1
Physical attack	2
Reported	1
Inappropriate contact with defendant's significant other	1
Alleged contract hit	1
<b>Total</b>	<b>29</b>

N=29

- 13) For any threats that you or an immediate family member received since January 2006, was the threat related to a specific case to which you were assigned?

<b>Yes/No</b>	<b>Number</b>	<b>Percentage</b>
Yes	51	84%
No	8	13%
Don't know	2	3%
<b>Total</b>	<b>61</b>	<b>100%</b>

- 14) Please specify the type of case to which you were assigned. (Check all that apply.)

<b>Case Type</b>	<b>Number of Responses</b>
Drugs	15
Gangs	9
Pro se (criminal defendant)	2
Pro se (civil defendant)	3
Public corruption	2
Terrorism	1
Tax (civil)	1
Tax (criminal)	1
Other	25
<b>Total</b>	<b>59</b>

N=51

Respondents could select more than one response.

Twenty-five respondents chose "Other" and provided answers in their own words. The OIG categorized information within their answers as follows:

<b>Case Type</b>	<b>Number of Responses</b>
Armed bank robbery	1
Assault/civil rights	1
Child exploitation	1
Civil rights violation	2
Collection	1
Drugs & gangs	1
Espionage & violent crime	1
Extortion	1
Felon in possession	2
Firearms	1
Firearms & child pornography	1
Foreign request for assistance	1
Fraud	1
Identity theft	1
Immigration	1
Postal	1
Project safe neighborhoods	1
Stalking	1
Violent crime	2
White collar	2
<b>Total</b>	<b>24</b>

N=25

One respondent answered with a number, not a case type.

- 15) If you answered “Other” to the previous question, please specify whether the case was civil or criminal.

<b>Civil/Criminal</b>	<b>Number of Responses</b>
Civil	1
Criminal	20
<b>Total</b>	<b>21</b>

N=21

Only 21 of 25 respondents who reported handling an “Other” case type in Question 14 answered this question.

- 16) Have you reported any threat(s) made against you personally or against a member of your family during your time as a U.S. Attorney or AUSA since January 2006?

<b>Yes/No</b>	<b>Number</b>	<b>Percentage</b>
Yes	51	84%
No	10	16%
<b>Total</b>	<b>61</b>	<b>100%</b>

- 17) Of the times that you, or a member of your family, were threatened since January 2006, how often did you report those threats? (Select one.)

<b>Threat Reported</b>	<b>Number</b>	<b>Percentage</b>
Every time	47	92%
Most of the time - half or more than half of the times you were threatened	4	8%
Some of the time - less than half of the times you were threatened	0	0%
Never	0	0%
<b>Total</b>	<b>51</b>	<b>100%</b>

- 18) If you only reported the threats most of the time or some of the time, what was/were your reason(s) for not reporting a threat? (Check all that apply.)

<b>Reason Not Reported</b>	<b>Number</b>	<b>Percentage</b>
I did not think the threat posed a real danger	3	75%
I was not familiar with the reporting procedures	0	0%
Threat reporting procedures were too cumbersome or inconvenient	0	0%
I did not want additional protection	0	0%
I did not feel that the protection provided would be adequate based on previous experience with the protection that was provided	1	25%
Other (please specify)	0	0%
<b>Total</b>	<b>4</b>	<b>100%</b>

19) If you never reported any threat(s) you received, why not? (Check all that apply.)

See Question 17. All of the survey respondents stated that they reported threats they received all or most of the time.

20) Since January 2006, when you reported your threat(s), to whom, and how often, did you report them? (Check all that apply.)

Entity Reporting To	Frequency of Reporting Threats to Entity			
	All of the Time	Most of the Time	Some of the Time	Never
District Office Security Manager	32	4	-	15
Other USAO managers	42	2	-	7
USMS	31	-	3	17
FBI	19	2	2	28
State or local law enforcement	8	1	3	39
Other	-	-	1	-

Missing column values indicate that no respondents chose that answer. One respondent reported the threat to ATF.

21) Please explain why you reported your threat(s) to the entity(s) you checked.

Reason Reported to Entity	Number of Responses
Regulation	15
Supervisor/chain of command	7
Protection/safety of self and family	4
Third party government employee informed threatenee	4
Reported to case agent	1
Described how the threats occurred	5
No answer	4
Miscellaneous	11
<b>Total</b>	<b>51</b>

N=51

22) Once your threat was reported, was a threat assessment done?

<b>Yes/No</b>	<b>Number</b>	<b>Percentage</b>
Yes	34	67%
No	4	8%
Don't know	13	25%
<b>Total</b>	<b>51</b>	<b>100%</b>

23) Were you given the results of the threat assessment?

<b>Yes/No</b>	<b>Number</b>	<b>Percentage</b>
Yes	24	71%
No	9	26%
Don't recall	1	3%
<b>Total</b>	<b>34</b>	<b>100%</b>

24) Please explain below why you believe that the threat assessment was or was not accurate or useful.

<b>Category</b>	<b>Number of Responses</b>
Threat was not serious	2
Threat was serious	4
Threateners were interviewed	2
Improved security	4
Useful	2
Accurate	3
USMS mitigated threat	2
Home alarm provided	1
Not useful	2
Appropriate feedback	1
<b>Total</b>	<b>23</b>

N=22

Only 22 of 24 respondents who reported receiving the results of the threat assessment in Question 23 answered this question.

One respondent provided more than one response.

25) After you reported the threat(s), what was the longest response time for each of the following entities? (Check all that apply.)

<b>Responding Entity</b>	<b>0-3 hours</b>	<b>3-12 hours</b>	<b>12-24 hours</b>	<b>1-3 days</b>	<b>Don't know</b>
District Office Security Manager	22	5	0	2	22
Other USAO managers	33	5	0	2	11
USMS	22	3	4	5	17
FBI	9	2	1	3	36
State or local law enforcement	6	1	1	1	42
Other	2	0	0	1	0

N=51

Three respondents chose “Other” and provided answers in their own words. The OIG categorized information within their answers as follows:

<b>Other Responding Entities</b>	<b>Number of Responses</b>
ATF	2
Customs and Border Patrol	1
Federal authorities not involved	1
<b>Total</b>	<b>4</b>

N=4

One respondent did not answer “Other” in Question 25, but responded to this question.

26) If other entities who are not listed in Question 25 responded to your threat, please specify which entities responded and their longest response time.

Of the three respondents who indicated an entity, two reported that the ATF responded within zero to three hours and the other respondent reported that Customs and Border Patrol responded within one to three days.

27) Since January 2006, when you reported the threat(s) that you or your family received, were you afforded any protective measures?

<b>Response</b>	<b>Number</b>	<b>Percentage</b>
Never	29	57%
Some of the time	5	10%
Most of the time	2	4%
All of the time	15	30%
<b>Total</b>	<b>51</b>	<b>100%</b>

28) Since January 2006, when you reported the threat that you or your family received, what [REDACTED] were you or your family offered? (Check all that apply.)

<b>Protective Measure</b>	<b>Not Offered</b>	<b>Offered But Declined</b>	<b>Offered And Accepted</b>
[REDACTED]			

N= [REDACTED]



29) If you were offered [REDACTED] other than those listed above, please specify what those measures were and whether you accepted or declined them.

Other Protective Measures Offered	Number of Responses
[REDACTED]	[REDACTED]
<b>Total</b>	[REDACTED]

N= [REDACTED]

30) Please indicate whether the investigation(s) and the protective measures provided by the U.S. Marshals Service in response to the threat(s) were appropriate.

USMS Measures Appropriate	Number	Percentage
[REDACTED]	[REDACTED]	[REDACTED]
<b>Total</b>	[REDACTED]	[REDACTED]

31) Please explain why you believe that the investigation and protective measures provided by the U.S. Marshal Service were or were not appropriate.

Appropriateness of USMS Response	Number of Responses
[REDACTED]	[REDACTED]
<b>Total</b>	[REDACTED]

N= [REDACTED]

32) Please indicate whether the investigation(s) and the protective measures provided by the EOUSA in response to the threat(s) were appropriate.

<b>EOUSA Measures Were Appropriate</b>	<b>Number</b>	<b>Percentage</b>
<b>Total</b>		

33) Please explain why you believe that the investigation and protective measures provided by the EOUSA were or were not appropriate.

<b>Reasons Why EOUSA Response Was or Was Not Appropriate</b>	<b>Number of Responses</b>
<b>Total</b>	
N=	

34) If you believe any of the [REDACTED] in Question 28 or Question 29 needed improvement, please explain below.

<b>Protective Measures That Need Improvement</b>	<b>Number of Responses</b>
[REDACTED]	[REDACTED]
<b>Total</b>	[REDACTED]

N=[REDACTED]

35) If you did not receive protective measures in response to a threat and you believe that you should have, please explain below.

<b>Reason Respondent Should Have Received Protective Measures</b>	<b>Number of Responses</b>
[REDACTED]	[REDACTED]
<b>Total</b>	[REDACTED]

N=[REDACTED]

**Daily Security Measures Provided**

36) Where is your office located?

<b>Location</b>	<b>Number</b>	<b>Percentage</b>
[REDACTED]	[REDACTED]	[REDACTED]
<b>Total</b>	[REDACTED]	[REDACTED]

37) If your office is NOT in a federal courthouse or federal building, which of the following [REDACTED] are used for building security? (Check all that apply or check "don't know" if you are not familiar with the security measures used in your building.)

**Non-Federal Facility**

<b>Building Security Feature</b>	<b>Number</b>	<b>Percentage (of 129)</b>
[REDACTED]		

[REDACTED]

**Non-Federal Facility**

<b>Additional Security Measures</b>	<b>Number of Responses</b>
[REDACTED]	
<b>Total</b>	[REDACTED]

N= [REDACTED]

38) How useful do you find the following building security measures?  
(Check N/A if you are not aware that your building has a particular measure)

**Non-Federal Facility**

<b>Security Measures</b>	<b>Not Useful</b>	<b>Somewhat Useful</b>	<b>Neutral</b>	<b>Useful</b>	<b>Very Useful</b>	<b>N/A</b>

N=

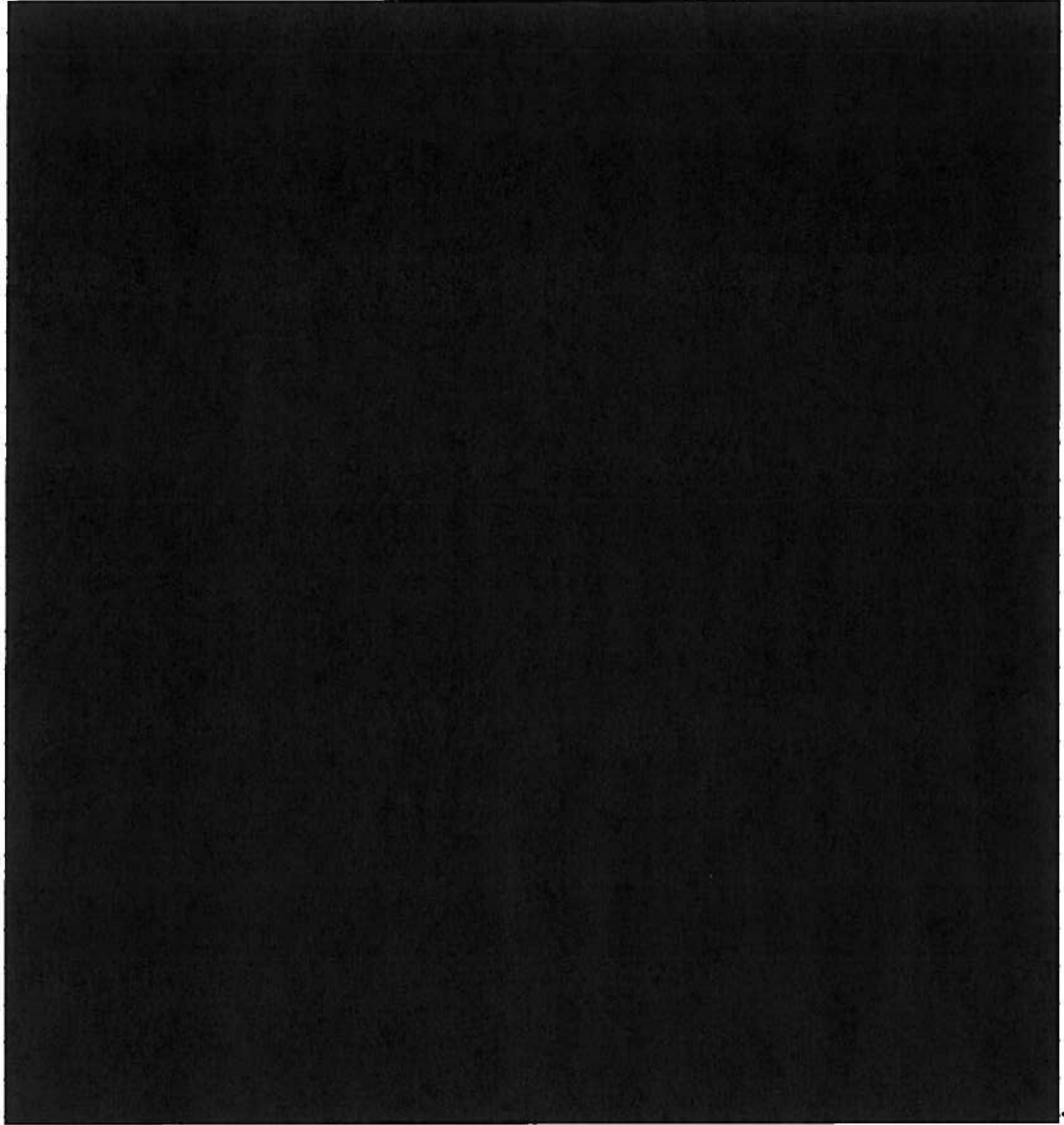
39) If you are aware of other building security measures not mentioned above, please specify what those measures are and whether you find them useful.

**Non-Federal Facility**

<b>Other Building Security Measures</b>	<b>Not Useful</b>	<b>Somewhat Useful</b>	<b>Neutral</b>	<b>Useful</b>	<b>Very Useful</b>	<b>Did Not Specify Usefulness</b>

N=

•



40) If you checked any of the building [REDACTED] in Question 38 as not useful, please explain.

**Non-Federal Facility**

<b>Reasons Building Security Measures Are Not Useful</b>	<b>Number of Responses</b>
[REDACTED]	
<b>Total</b>	

N=X

41) If your office IS in a federal courthouse or federal building, which of the following security measures are used for building security? (Check all that apply or check "don't know" if you are not familiar with the security measures used in your building.)

**Federal Facility**

<b>Building Security Feature</b>	<b>Number</b>	<b>Percentage (of 254)</b>
[REDACTED]		

[REDACTED]

**Federal Facility**

<b>Other Security Measures</b>	<b>Number of Responses</b>
<b>Total</b>	
N=	

42) How useful do you find the following building [REDACTED]? (Check N/A if you are not aware that your building has a particular measure)

**Federal Facility**

<b>Security Feature</b>	<b>Not Useful</b>	<b>Somewhat Useful</b>	<b>Neutral</b>	<b>Useful</b>	<b>Very Useful</b>	<b>N/A</b>



43) If you are aware of other building [REDACTED] not mentioned above, please specify what those measures are and whether you found them useful.

**Federal Facility**

Other Building Security Measures	Not Useful	Somewhat Useful	Neutral	Useful	Very Useful	Did Not Specify Usefulness
[REDACTED]						

N= [REDACTED]

44) If you checked any of the building security measures in Question 42 as not useful, please explain.

**Federal Facility**

Reasons Building Security Measures Are Not Useful	Number of Responses
[REDACTED]	
<b>Total</b>	[REDACTED]

N= [REDACTED]

45) Are there any other [REDACTED] you believe should be taken in terms of building security? Please explain below.

<b>Needed Building Security Measures</b>	<b>Number of Responses</b>
[REDACTED]	
<b>Total</b>	[REDACTED]
N=	[REDACTED]

46) Does your office provide parking?

<b>Location of Parking</b>	<b>Number of Responses</b>
[REDACTED]	
N=	[REDACTED]

47) What features does the parking facility have? (Check all that apply.)

<b>Parking Security Features</b>	<b>Number of Responses</b>
[REDACTED]	
N=	[REDACTED]

[REDACTED] and provided answers in their own words. The OIG categorized information within their answers as follows:

Other Parking Security Measures	Number of Responses
[REDACTED]	
<b>Total</b>	[REDACTED]
N= [REDACTED]	

48) If you think the security of your office's parking facility needs improvement, please explain below.

Needed Parking Improvements	Number of Responses
[REDACTED]	
<b>Total</b>	[REDACTED]
N= [REDACTED]	

49) Are there any other [REDACTED] you believe should be taken in terms of parking facility security? Please explain below.

<b>Additional Parking Measures Needed</b>	<b>Number of Responses</b>
[REDACTED]	
<b>Total</b>	[REDACTED]
N=	[REDACTED]

50) Do you have a [REDACTED]?

	<b>Number</b>	<b>Percentage</b>
[REDACTED]		
<b>Total</b>	[REDACTED]	[REDACTED]

51) Do you believe that [REDACTED] should be offered as a routine protective measure?

<b>Yes/No</b>	<b>Number</b>	<b>Percentage</b>
[REDACTED]		
<b>Total</b>	[REDACTED]	[REDACTED]

52) Please explain why you believe that [REDACTED] should or should not be offered as a routine protective measure.

[REDACTED]

<b>Reasons [REDACTED] Should Be a Routine Protective Measure</b>	<b>Number of Responses</b>
[REDACTED]	[REDACTED]
<b>Total</b>	[REDACTED]

<b>Reasons [REDACTED] Should Not Be a Routine Protective Measure</b>	<b>Number of Responses</b>
[REDACTED]	[REDACTED]
<b>Total</b>	[REDACTED]

**Security Training**

53) Have you received personal security training at the USAO (either in person, by PowerPoint presentation, or other means)?

<b>Security Training</b>	<b>Number</b>	<b>Percentage</b>
Received security training	291	76%
Did not receive security training	55	14%
Don't recall if received security training	37	10%
<b>Total</b>	<b>383</b>	<b>100%</b>

54) How long after you were initially employed at the USAO did you receive the security training (either in person or by other means)?

<b>Elapsed Time From Initial Employment to Security Training</b>	<b>Number</b>	<b>Percentage</b>
Within the first month	71	24%
Within the first 3 months	6	2%
Within the first 6 months	19	7%
Within the first year	26	9%
Sometime after the first year of employment	53	18%
Don't remember when training received	116	40%
<b>Total</b>	<b>291</b>	<b>100%</b>

55) As part of your initial security training, did you receive instructions to follow if you receive a threat?

<b>Yes/No</b>	<b>Number</b>	<b>Percentage</b>
Yes	220	76%
No	12	4%
Don't know	59	20%
<b>Total</b>	<b>291</b>	<b>100%</b>

56) Have you received subsequent personal security training as a refresher (either in person, by PowerPoint presentation, or by other means)?

<b>Yes/No</b>	<b>Number</b>	<b>Percentage</b>
Yes	217	75%
No	47	16%
Don't know	27	9%
<b>Total</b>	<b>291</b>	<b>100%</b>

57) Did your security training address any of the following topics? (Check all that apply.)

<b>Security Training Topic</b>	<b>Number of Responses</b>	<b>Percentage (out of 291)</b>
Home security	122	42%
Work-related travel	195	67%
Driving	124	43%
Commuting	128	44%
Emergency contact numbers	199	83%
Other	21	7%
None of the above	41	14%

N=291

Twenty-one respondents chose 'Other' and provided answers in their own words. The OIG categorized information within their answers as follows:

<b>Other Topics Covered in Security Training</b>	<b>Number of Responses</b>
Courtroom security	3
Additional aspects of work-related travel	1
Threats	2
Don't recall	7
<b>Total</b>	<b>23</b>

N=21

Some respondents provided more than one response.

58) How useful did you find the security training provided in the following areas? (Check "N/A" if you did not receive training in an area.)

<b>Security Topic</b>	<b>Not Useful</b>	<b>Somewhat Useful</b>	<b>Neutral</b>	<b>Useful</b>	<b>Very Useful</b>	<b>N/A</b>
Home security	15	19	24	73	19	141
Work-related traveling	16	28	29	107	27	84
Driving	12	22	24	76	19	138
Commuting	13	26	25	69	17	141
24-hour emergency contact numbers	7	16	22	108	72	66
Initial security briefing	10	25	32	119	37	68
Subsequent refresher training	10	20	34	104	36	87
Training on threat procedures	6	25	32	124	38	66

N=291

59) If you think any of the security training or briefings provided in your office need improvement, please explain below.

<b>Security Topics That Need Improvement</b>	<b>Number of Responses</b>
Residential and commuting topics	18
Refresher training	11
Overall training content	14
Parking information	3
Preventing and deterring threats	1
Miscellaneous	8
<b>Total</b>	<b>56</b>

N=54

Some respondents provided more than one response.



60) Are there any other measures you believe the training should address in terms of personal safety? Please explain below.

Additional Training Needed	Number of Responses
[REDACTED]	
<b>Total</b>	

N= [REDACTED]

61) Does the District Office Security Manager make websites, brochures, or videotapes on security topics easily available to you?

Yes/No	Number	Percentage
Yes	136	36%
No	68	18%
Don't know	179	47%
<b>Total</b>	<b>383</b>	<b>100%</b>

62) Do you find these websites, brochures, or videotapes on security topics useful?

Usefulness of Websites, Brochures, or Videotapes	Number	Percentage
Not useful	6	4%
Somewhat useful	22	16%
Neutral	43	32%
Useful	57	42%
Very useful	8	6%
<b>Total</b>	<b>136</b>	<b>100%</b>

63) Please explain below why you find these resources to be useful or not useful.

<b>Reasons Resources Are or Are Not Useful</b>	<b>Number of Responses</b>
Information is too general in nature	7
Information is useful and relevant	8
DOSM provides current security information to the USAO	4
Information is a good refresher	4
Comments discuss topics covered in the training	3
Have not reviewed the materials	2
Materials not always consulted	2
Useful once received training as a U.S. Attorney	1
Have to request materials in order to review them	1
Too much information provided	1
<b>Total</b>	<b>33</b>

N=30

Some respondents provided more than one response.

**APPENDIX IV: THE UNITED STATES MARSHALS SERVICE'S  
RESPONSE**

---



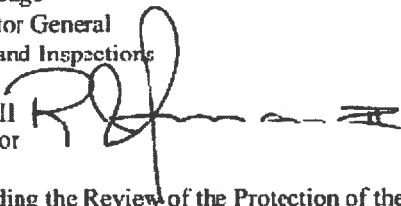
U.S. Department of Justice  
United States Marshals Service  
*Operations Directorate*

---

*Alexandria, Virginia 22301-1625*

December 16, 2009

MEMORANDUM TO: Michael D. Gulledge  
Assistant Inspector General  
for Evaluation and Inspections

FROM: Robert J. Finan, II   
Associate Director

SUBJECT: Response Regarding the Review of the Protection of the Judiciary  
and the United States Attorneys, Assignment Number A-2008-006

This is in response to your correspondence seeking comment on the draft subject report. Attached please find the USMS response to the applicable recommendations.

Should you have any questions, please contact Ms. Isabel Howell, Audit Liaison, at 202-307-9744.

Attachment

cc: Isabel Howell  
External Audit Liaison  
United States Marshals Service

Richard P. Theis  
Assistant Director, Audit Liaison Group  
Justice Management Division

**USMS Response to Draft Recommendations**

**Recommendation 1) The USMS clearly explain to protectees the detrimental effect that delays or the failure to report has on the security provided.**

**Response:** Concur

The USMS constantly interacts with protectees and emphasizes the need for immediate reporting of threats, inappropriate communications, and other security issues. The USMS also emphasizes to its employees the importance of communication with, and support of, federal prosecutors who receive inappropriate communications and/or threats. Specifically, Protective Intelligence Investigators (PIIs), District Threat Investigators (DTIs), and Judicial Security Inspectors (JSIs) receive training that explains the role of the District Office Security Manager (DOSM) within the United States Attorneys Office (USAO), and further emphasizes the significance of maintaining a close working relationship with the DOSM. The USMS also regularly provides training to the court family, to include USAO, on issues that include off-site security, personal security, and timely threat reporting. These training sessions utilize a number of resources, including USMS Publication 94, *Off-Site Security for Judges, United States Attorneys, and Their Families*, USMS Publication 6, *Personal Security Handbook*, and a Department of Justice, National Institute of Justice (DOJ/NIJ) publication, *Protective Intelligence and Threat Assessment Investigations*.

Through coordination with the Administrative Office of the United States Courts (AOUSC), the USMS also provides security presentations during Judicial Nominee Briefings and New Chief Judge Orientations. During these presentations, the USMS stresses security issues and provides copies of USMS Publications 6 and 94. When Judges update Form USM 50, *Judicial Personnel Profile*, the USMS emphasizes the importance of reporting threats and inappropriate communications. The USMS has also begun emphasizing the importance of threat reporting through presentations at magistrate judges conferences, judicial conferences, and at Judicial Security Committee meetings.

The USMS will continue to emphasize the need for immediate reporting of threats, inappropriate communications, and security issues whenever an opportunity arises.

**Recommendation 2) The USMS update its security handbook to emphasize both the importance of immediately reporting threats to the USMS and the consequences of delays or failures to report.**

**Response:** Concur

USMS Publication 94 is widely distributed both to the Judiciary and USAOs. Publication 94 was last edited and updated for distribution in December 2008. The USMS is currently collecting information to make necessary edits for a future edition. Future revisions to Publication 94 will include verbiage emphasizing the importance of immediately reporting threats and inappropriate communications to the USMS, as well as the consequences of delaying or failing to report these issues.

**Recommendation 3) EOUSA**

**Recommendation 4) The USMS review trends in reporting timeliness annually and provide results of that analysis to the Administrative Office of the U.S. Courts (AOUSC) and the EOUSA for their use in judicial conferences and attorney conferences.**

**Response: Concur**

The USMS will review trends in reporting timeliness annually and provide results of that analysis to AOUSC and EOUSA for use in judicial and attorney conferences.

**Recommendation 5) The USMS implement controls to ensure that required risk assessments are completed and documented in the USMS threat database, including the assignment of risk levels, and that the protective measures provided in response to each threat also be documented in the USMS threat database.**

**Response: Concur**

The USMS conducts protective investigations using the behavior based approach to assess the threat and assign a risk level. DTIs/PIIs in the field notify the USMS Threat Management Center (TMC) and receive support in the form of recommendations and analysis. For low and potential risk cases, the case is designated as "standard." For high risk cases, the DTIs/PIIs assign the priority rating of "expedite" to the Form USM 550, *Preliminary Threat Report* to identify the urgency for analysis. As the protective investigation progresses, the facts and behavior that are developed may change, and are documented on a Form USM-11, *Investigative Report*. Because the risk level changes during the investigation, either escalating or deescalating, no fixed risk level is entered into the Justice Detainee Information System (JDIS).

The District Judicial Security Inspector (JSI) is responsible for recommending and coordinating the protective response. The JSI and the DTI/PII then consult with district management to identify the appropriate protective measures and the protective response. The JSI frequently coordinates the protective response with USMS Headquarters.

As a result of this process, risk levels are communicated between the DTI/PII, the JSI, and district management so that protective responses help ensure the safety of our protectees. Unfortunately there is no way to quantify how many attacks have been prevented through this process.

The USMS is revising the *Guide to Protective Investigations and Contemporary Threat Management*, a working guide and instruction manual for DTIs/PIIs that was last revised in 2008. The USMS is also revising its Policy Directive 10, *Judicial and Court Security*. This policy directive was last revised in 2006. Following these revisions, both documents will provide consistent instruction and guidance concerning risk assessments and the assignment of risk levels.

**Recommendation 6) Establish internal controls at USMS Headquarters to ensure that the USMS database contains full and accurate information, including ensuring that district offices regularly enter data in the “FBI notified” and “Notification Date” fields.**

**Response:** Concur

The USMS will strengthen existing internal controls at USMS Headquarters to ensure that the USMS database, the Justice Detainee Information System (JDIS), contains full and accurate information.

The USMS will adjust JDIS to reflect both notification of the FBI (date, location, and Special Agent) on a threat, as well as non-notification of the FBI when an inappropriate communication has been reported but does not rise to the level of prosecutorial investigation. The current database only allows the district to report when and where notification of the FBI was accomplished, and does not take into account the numerous cases that have no prosecutorial merit, including nuisance calls, repetitive pro se filing, inappropriate attraction, and others.

The current internal controls consist of personnel in the Threat Management Center (TMC) reviewing all cases as they are entered into JDIS by the district. Once the change discussed above is made in the JDIS database, the USMS will provide additional direction to the field, as well as additional training for TMC personnel, to ensure each case is thoroughly completed.

Per USMS Directive 10.3, *Protective Investigations*, all threats are inappropriate communications, but not all inappropriate communications are threats. In this review, the OIG used the term threat to encompass both threats and inappropriate communications, and did not differentiate between the two. Per USMS Directive 10.3, section E.l.c., “Report to Office of Protective Intelligence (OPI) Duty Desk: In the event of a threat or inappropriate communication, district managers will immediately report the situation to the OPI duty desk and the local office of the FBI (if the inappropriate communication contains a threat).”

**Recommendation 7) Coordinate with the FBI to establish a memorandum of understanding to formalize the coordination of protective and criminal investigations.**

**Response:** Concur

The USMS will consult with the FBI about establishing a memorandum of understanding to formalize the coordination of protective and criminal investigations.

**Recommendation 8) Develop a mechanism to track the USMS district office responses to emergency notifications from local law enforcement agencies regarding emergency responses to federal judges’ residences.**

**Response:** Concur

The USMS is developing a mechanism to track USMS district office responses to emergency notifications from local law enforcement agencies regarding emergency responses to federal judges' residences.

**Recommendation 9) Ensure that all districts send the required notification letters to local law enforcement agencies and that the letters contain a working contact number that connects directly to the local USMS duty officer.**

**Response:** Concur-in part

The USMS requires that all districts send notification letters to local law enforcement agencies. This is tracked within a USMS database that lists all federal judges. A new memorandum will be issued that clearly explains that the notification letters contain a working contact number that connects directly to the local USMS office. After business hours, the USMS answering service, which is often an area law enforcement agency, will contact the USMS Duty Officer. As USMS Duty Officers rotate frequently, it is impractical and unnecessary to have the number connect "directly to the local USMS duty officer" as they may be transferred, on vacation, or on leave.

It is believed that this finding of non-working numbers was primarily driven by the past issuance of a "working contact number that connects directly to the local USMS duty officer." The problem would continue if contact numbers were issued in this fashion, and we cannot support it.

The USMS agrees that it is critically important that the notification letter must list a working contact number for the local USMS office, and have connectivity to the local USMS Duty Officer at all times.

**Recommendation 10) EOUSA**

**Recommendation 11) The USMS and EOUSA sign a MOU that defines their roles and responsibilities in protecting U.S. Attorneys and AUSAs who receive threats.**

**Response:** Concur

The USMS will consult with EOUSA about establishing a memorandum of understanding that defines their roles and responsibilities in protecting United States Attorneys and Assistant United States Attorneys who receive threats.

**Recommendation 12) EOUSA**

**Recommendation 13) EOUSA**

**Recommendation 14) EOUSA**

**APPENDIX V: OIG'S ANALYSIS OF THE UNITED STATES  
MARSHALS SERVICE'S RESPONSE**

---

The Office of the Inspector General provided a draft of this report to the United States Marshals Service (USMS) for its comment. The report contained 14 recommendations: Recommendations 1, 2, 4, and 5 through 9 are directed to the USMS. Recommendations 3, 10, 12, 13, and 14 are directed to the Executive Office for United States Attorneys (EOUSA). Recommendation 11 is directed to both the USMS and EOUSA.

The USMS's response is included in Appendix IV to this report. The OIG's analysis of the USMS's response and the actions necessary to close the recommendations are discussed below.

**Recommendation 1.** The USMS clearly explain to protectees the detrimental effect that delays or the failure to report has on the security provided.

**Status.** Resolved – open.

**Summary of USMS Response.** The USMS concurred with this recommendation. According to the USMS, it already emphasizes to protectees the need for immediate reporting of threats, inappropriate communications, and other security issues. The USMS stated that it regularly provides training to federal court officials, including United States Attorney's Office (USAO) staff, on issues that include off-site security, personal security, and timely threat reporting.

The USMS further stated in its response that through coordination with the Administrative Office of the U.S. Courts (AOUSC), it provides security presentations during Judicial Nominee Briefings and New Chief Judge Orientations. According to the USMS, it stresses security issues during these presentations and provides copies of USMS security publications. The USMS stated that when judges update their judicial personnel profiles, the USMS emphasizes the importance of reporting threats and inappropriate communications. According to the USMS, it has also begun emphasizing the importance of threat reporting through presentations at magistrate judges' conferences, judicial conferences, and Judicial Security Committee meetings. The USMS stated that it will continue to emphasize the need for immediate reporting of threats, inappropriate communications, and security issues whenever an opportunity arises.



**OIG Analysis.** The actions taken by the USMS are partially responsive to our recommendation. The USMS has described the training it provides to the judges, but did not mention training for attorneys. Please provide the OIG, by March 1, 2010, with copies of the security presentations from Judicial Nominee Briefings, New Chief Judge Orientations, magistrate judges' conferences, judicial conferences, and a sample of the presentations from the Judicial Security Committee meetings for fiscal year (FY) 2009. Also please provide a list of the training provided to the other federal court officials, including the attorneys, and copies of the training presentations.

**Recommendation 2.** The USMS update its security handbook to emphasize both the importance of immediately reporting threats to the USMS and the consequences of delays or failures to report.

**Status.** Resolved – open.

**Summary of USMS Response.** The USMS concurred with this recommendation and stated that it is currently collecting information to edit its security handbook, *Off Site Security for Judges, United States Attorneys and their Families*, which was last updated in December 2008. The USMS stated in its response that future revisions to this handbook will emphasize the importance of immediately reporting threats and inappropriate communications to the USMS, as well as the consequences of delaying or failing to report these incidents.

**OIG Analysis.** The actions proposed by the USMS are responsive to our recommendation. Please provide the OIG with an updated copy of the security handbook or a status report of the edits to the handbook by March 1, 2010.

**Recommendation 4.** The USMS review trends in reporting timeliness annually and provide the results of that analysis to the Administrative Office of the U.S. Courts and EOUSA for their use in judicial conferences and attorney training seminars.

**Status.** Resolved – open.

**Summary of USMS Response.** The USMS concurred with this recommendation. The USMS stated that it will review trends in reporting timeliness annually and provide the results of that analysis to AOUSC and EOUSA for use in judicial and attorney conferences.

**OIG Analysis.** The actions proposed by the USMS are responsive to our recommendation. Please provide the results of the analysis of the timeliness of threat reporting and the methods used to obtain the results by March 1, 2010.

**Recommendation 5.** The USMS implement controls to ensure that required risk assessments are completed and documented in the USMS threat database, including the assignment of risk levels, and that the protective measures provided in response to each threat also be documented in the USMS threat database.

**Status.** Resolved – open.

**Summary of USMS response.** The USMS concurred with this recommendation. However, the USMS stated that the risk level may change during the investigation and therefore no fixed risk level is entered into the threat database. According to the USMS, risk levels are communicated between the District Threat Investigator, the Protective Intelligence Investigator, the Judicial Security Inspector, and district management. The USMS is revising the *Guide to Protective Investigations and Contemporary Threat Management*, which is a working guide and instruction manual for District Threat Investigators and Protective Intelligence Investigators that was last revised in 2008. The USMS is also revising its Policy Directive 10, *Judicial and Court Security*, which was last revised in 2006. The USMS stated that following these revisions both documents will provide consistent instruction and guidance concerning risk assessments and the assignment of risk levels.

**OIG Analysis.** The intent of this recommendation was to ensure that the risk level and the protective measures are documented in the USMS threat database. If the risk level changes during the course of the threat response process, this change can be updated in the database. Without documentation of the risk level or the protective measures provided, the only way USMS headquarters can verify that the appropriate protective measures have been taken is to contact the districts and rely on the memory of district personnel.

In addition, in its response the USMS did not specify what instruction and guidance concerning risk assessments and the assignment of risk levels would be provided in the revision of the USMS directive and the instruction manual. Please provide a copy of the revised directive and instruction manual that shows that the risk level and protective measures provided are

to be documented in the USMS threat database or a status report on the progress of the revisions by March 1, 2010.

**Recommendation 6.** Establish internal controls at USMS headquarters to ensure that the USMS threat database contains full and accurate information, including ensuring that district offices regularly enter data in the “FBI Notified” and notification date fields.

**Status.** Resolved – open.

**Summary of USMS Response.** The USMS concurred with this recommendation and stated that it will strengthen existing internal controls at USMS headquarters to ensure that the threat database contains full and accurate information. The USMS will adjust the threat database to reflect both notification of the Federal Bureau of Investigation (FBI) of a threat, including the date, location, and Special Agent notified, as well as non-notification of the FBI when an inappropriate communication has been reported but does not rise to the level of a criminal investigation. Once the database is modified, the USMS will provide additional direction to the field, as well as additional training for headquarters personnel, to ensure each case is thoroughly completed.

**OIG Analysis.** The actions proposed by the USMS are responsive to our recommendation. Please provide, by March 1, 2010, a screen capture of the threat database showing the changes made to the database, showing notification of the FBI of a threat, including the date, location, and Special Agent notified, as well as non-notification of the FBI when an inappropriate communication has been reported but does not rise to the level of a criminal investigation. In addition, please provide the internal controls to be implemented to ensure that this data is recorded.

**Recommendation 7.** Coordinate with the FBI to establish a memorandum of understanding to formalize the coordination of protective and criminal investigations.

**Status.** Resolved – open.

**Summary of USMS Response.** The USMS concurred with the recommendation and stated that it will consult with the FBI about establishing a memorandum of understanding to formalize the coordination of protective and criminal investigations.

**OIG Analysis.** The action proposed by the USMS is responsive to our recommendation. Please provide a copy of the memorandum of understanding between the USMS and the FBI formalizing the coordination of protective and criminal investigations, or a status report of the progress in establishing the memorandum, by March 1, 2010.

**Recommendation 8.** Develop a mechanism to track the USMS district office responses to emergency notifications from local law enforcement agencies regarding emergency responses to federal judges' residences.

**Status.** Resolved – open.

**Summary of USMS Response.** The USMS concurred with our recommendation and stated that it is developing a mechanism to track USMS district office responses to emergency notifications from local law enforcement agencies.

**OIG Analysis.** The action proposed by the USMS is responsive to our recommendation. Please provide a description of the mechanism that the USMS will use to track its district office responses to emergency notifications from local law enforcement agencies, or a status report on the creation of this mechanism, by March 1, 2010.

**Recommendation 9.** Ensure that all districts send the required notification letters to local law enforcement agencies and that the letters contain a working contact number that connects directly to the local USMS duty officer.

**Status.** Resolved – open.

**Summary of USMS Response.** The USMS concurred in part with this recommendation. In its response, the USMS stated that it requires all districts to send notification letters to local law enforcement agencies and tracks in its database whether this notification is done. The USMS will issue a new memorandum that clearly explains that the notification letters are to contain a working contact number that connects directly to the local USMS office. After business hours, the USMS answering service, which is often an area law enforcement agency, will receive the calls and contact the USMS duty officer. The USMS stated that because USMS duty officers rotate frequently, it is impractical and unnecessary to have the number connect directly to them as they may be transferred, on vacation, or on leave. The USMS also stated that it believed that the OIG finding of non-working numbers was primarily driven by the past issuance of a working

contact number that connected directly to the local USMS duty officer. According to the USMS, the problem would continue if contact numbers were issued in this fashion, and it cannot support the part of the OIG recommendation to require that the letters contain a working contact number that connects directly to the local USMS duty officer. However, the USMS agreed that it is critically important that the notification letter list a working contact number for the local USMS office and have connectivity to the local USMS duty officer at all times.

**OIG Analysis.** The intent of this recommendation is to ensure that the USMS is notified promptly if an emergency occurs at a judge's residence. The USMS has provided a viable explanation for its partial non-concurrence with this recommendation, and we accept the proposed alternative procedure. Please provide the OIG, by March 1, 2010, a copy of the new memorandum that clearly explains that the notification letters must contain a working contact number that connects directly to the local USMS office or the USMS answering service after business hours. Please also provide the OIG some copies of letters the districts send to the local law enforcement agencies in their districts that contain a working number that connects directly to the local USMS office or the USMS answering service after business hours.

**Recommendation 11.** The USMS and EOUSA sign a memorandum of understanding that defines their roles and responsibilities in protecting U.S. Attorneys and AUSAs who receive threats.

**Status.** Resolved – open.

**Summary of USMS Response.** The USMS concurred with the recommendation. The USMS will consult with EOUSA about establishing a memorandum of understanding that defines their roles and responsibilities in protecting United States Attorneys and AUSAs who receive threats.

**OIG Analysis.** The actions planned by the USMS are responsive to our recommendation. Please provide the OIG with a copy of the memorandum of understanding that describes the roles and responsibilities of EOUSA, USAOs, USMS headquarters, and USMS district offices by March 1, 2010.

APPENDIX VI: THE EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS' RESPONSE



U.S. Department of Justice

Executive Office for United States Attorneys  
Office of the Director

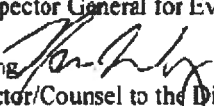
Main Justice Building, Room 2261  
956 Pennsylvania Avenue, NW  
Washington, DC 20537

(202) 514-212A

MEMORANDUM

DATE: December 11, 2009

TO: Michael Gullede  
Assistant Inspector General for Evaluations and Inspections

FROM: Norman Wong   
Deputy Director/Counsel to the Director  
Executive Office for United States Attorneys

SUBJECT: Response to OIG's Report Entitled: Review of the Protection of the Judiciary and the United States Attorneys, A-2008-006

This memorandum is submitted by the Executive Office for United States Attorneys (EOUSA) in response to the audit report by the Office of Inspector General (OIG) entitled, "Review of the Protection of the Judiciary and the United States Attorneys," Report No. A-2008-006.

The safety and security of each and every employee within the United States Attorneys' Offices (USAOs), and within EOUSA, are of paramount importance to EOUSA and the USAOs. EOUSA welcomes and appreciates this review regarding the procedures used to help protect United States Attorneys and Assistant United States Attorneys. We believe the recommendations from the report will have a positive impact on the USAO community.

As the report makes clear, the number of threats to USAO personnel have been increasing since 2006. EOUSA currently has in place an effective and relatively efficient system for learning about, tracking, and helping to respond to threats to United States Attorneys and Assistant United States Attorneys. The system is based upon a threat reporting structure that starts with a report of a threat to the District Office Security Manager (DOSM) in a USAO. The DOSM then reports the threat to EOUSA, the United States Marshals Service, and the FBI, as appropriate.

Of course, the DOSM can only report threats of which he or she is aware. As the report makes clear, not all threats are being reported to the DOSMs, in part perhaps because the threatened individual does not consider the threat to be serious. As noted below in response to recommendation No. 3, EOUSA will continue to notify all USAO employees to promptly notify

the DOSM of any threat, regardless of whether the employee considers the threat to be serious. Reports of non-serious threats are still important in helping EOUSA coordinate with the USMS and FBI, and in giving those agencies a context and pattern to investigate any future threats. The report of non-serious threat may be critical in helping to prosecute a later, serious threat to the same or another employee.

The OIG report also notes that when reports of threat are made, they do not always include full and complete information regarding the threat, and that tracking follow-up activities undertaken in response to reported threats could be improved. Even prior to the OIG report recommendation on this issue, EOUSA had undertaken to convert the current Urgent Report system to a web-based reporting system. We expect that a web-based system will improve the completeness and timeliness of both initial reports of threat and follow-up reports.

The report also suggests additional training for both DOSMs and EOUSA personnel. EOUSA always welcomes and encourages additional training. We note our continued disagreement, however, with the characterization, on pages ii, v, and 27, regarding the level of expertise held by the current EOUSA security personnel. Unlike the DOSM positions in the USAOs, which are collateral duty positions and may properly be filled by persons with varying degrees of security experience, the security personnel at EOUSA, including the Assistant Director for Security Programs, have and properly should have extensive security-related backgrounds. We also strongly disagree with the statement on page 28 that the Assistant Director has limited time to devote to threat response and related training. The safety and security of USAO employees is always the Assistant Director's top priority.<sup>1</sup>

---

<sup>1</sup>EOUSA's Assistant Director has 29 years of federal security related experience with the United States Army, the Drug Enforcement Administration, and other agencies. Both as a Counterintelligence Technician (Special Agent) for the Department of the Army and later as Supervisory Physical Security Specialist with the DEA, he has undertaken residential security evaluations of individuals following their receipt of a threat. His evaluations included an assessment of the threat of criminal activity, such as burglaries, as well as more sophisticated intrusions such as electronic eavesdropping. As a Physical Security Specialist with the DEA, he developed, designed, and implemented intrusion detection, access control, and surveillance systems for both commercial and residential locations. He has served as an instructor with the US Army, DEA, the Department of Defense, and EOUSA on security-related topics, including physical security and risk management. He has attended, each year for the past 10 years, the American Society for Industrial Security (ASIS) annual conference, which is a 40 hour annual training event in various security disciplines. In addition, we note that the current Threat Management Specialist at EOUSA is a former Commander of the Technical Investigations Section of the Maryland State Police. In that role he supervised 20 investigators and analysts.

Recommendations

The recommendations below are numbered according to the numbers given them in the report.

3. *EOUSA amend the U.S. Attorneys' Manual to clearly instruct the AUSAs that all threats must be reported promptly to the District Office Security Manager. Such instruction should include an explanation of the detrimental effect that delays or the failure to report has on the security provided.*

EOUSA agrees to implement this recommendation. EOUSA has already, prior to a formal amendment of the USAM, issued a memorandum to all United States Attorneys reminding them that it is incumbent upon each Assistant United States Attorney and each USAO employee to notify the District Office Security Manager in their district of any and all threats, even if they do not believe that the threat is a serious one. The memorandum notes that the report of threat plays a critical role in helping the USMS assess the pattern and context of future threats. EOUSA is providing OIG with a copy of that memorandum under separate cover. In addition, EOUSA will notify OIG when the USAM has been formally amended.

10. *EOUSA provide, in consultation with the USMS, sufficient training to EOUSA and USAO staff assigned threat response.*

EOUSA agrees to implement this recommendation. EOUSA will consult with the USMS on the training curriculum.

11. *The USMS and EOUSA sign a memorandum of understanding that defines their roles and responsibilities in protecting U.S. Attorneys and AUSAs who receive threats.*

EOUSA agrees to implement this recommendation. While EOUSA and the USMS have a cooperative and effective relationship, a formal memorialization of the roles and responsibilities between EOUSA and the USMS when a threat is received by a USAO employee is appropriate. EOUSA will consult with USMS to produce the memorandum of understanding.

12. *EOUSA provide guidance and periodic reminders to USAOs of the requirement to submit Urgent Reports immediately when a U.S. Attorney or AUSA is threatened.*

EOUSA agrees to implement this recommendation. As noted above, EOUSA has already issued a memorandum to all United States Attorneys reminding all USAO employees to notify their DOSM and office management when a threat is received.



13. *EOUSA revise the Urgent Report template so that it includes a requirement to provide at least the following information:*
- *name and position of targeted employee;*
  - *name and location of the person making the threat, if known;*
  - *date the threat was made, or date the target was made aware of the threat;*
  - *date the District Office Security manager was informed of the threat;*
  - *date the USMS and FBI were notified; and*
  - *date the USAO submitted the Urgent Report to EOUSA*

EOUSA agrees to implement this recommendation. As indicated above and in the report, EOUSA is developing a new, web-based Urgent Report system that will facilitate more timely and complete threat reporting. EOUSA hopes to pilot the new web-based system in the second quarter of 2010. Also, as part of the memorandum issued to all United States Attorneys, referred to above, EOUSA has created and made available to all USAOs a new threat reporting form, to be used in the existing Urgent Report system. The new form covers all the information listed above.

14. *EOUSA establish guidance to require the District Office Security Managers to send updated information via Urgent Reports at regular intervals to inform EOUSA of the status of USAO, USMS, and FBI actions to protect the threatened AUSA.*

EOUSA agrees to implement this recommendation. The memorandum just issued to all United States Attorneys reminds each office of this requirement. Moreover, the new, web-based system will facilitate greater and more complete follow-up reporting from the districts.

**APPENDIX VII: OIG'S ANALYSIS OF THE EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS' RESPONSE**

---

The Office of the Inspector General provided a draft of this report to the Executive Office for United States Attorneys (EOUSA) for its comment. The report contained 14 recommendations: Recommendations 1, 2, 4, and 5 through 9 are directed to the United States Marshals Service (USMS). Recommendations 3, 10, 12, 13, and 14 are directed to EOUSA. Recommendation 11 is directed to both the USMS and EOUSA.

EOUSA's response is included in Appendix VI to this report. In its response, EOUSA concurred with the recommendations addressed to it, and outlined steps to address the recommendations. It also made general comments regarding statements in the report on the level of expertise of EOUSA security personnel. We first address EOUSA's comments and then discuss its response to the recommendations.

**General Comments**

**Summary of EOUSA Response.** EOUSA in its response disagreed with the OIG's characterization of the expertise of current EOUSA security personnel in judicial security operations. EOUSA stated that unlike the District Office Security Manager positions in the United States Attorney Offices (USAO), which are collateral duty positions and may be filled by persons with varying degrees of security experience, the security personnel at EOUSA, including the Assistant Director for Security Programs, have extensive security-related backgrounds. EOUSA also stated in response to the OIG's statement on page 28 of the report that the safety and security of USAO employees is always the Assistant Director's top priority.

**OIG Analysis.** OIG agrees that the Assistant Director of the Security Programs Staff has an extensive background in physical and electronic and security operations appropriate to fulfill his role overseeing many of the security related matters facing USAOs. However, Deputy Marshals involved in ensuring the safety of protectees generally have not only extensive law enforcement training, but also specific training in protecting members of the judiciary, including determining and implementing threat response procedures. Moreover, our concern was primarily with the experience and training of the USAO staff in the 93 judicial districts, since they are the on-site personnel responding directly when United States Attorneys and Assistant United States Attorneys (AUSA) are threatened.

**Recommendation 3.** EOUSA amend the *U.S. Attorneys' Manual* to clearly instruct the AUSAs that all threats must be reported promptly to the District Office Security Manager. Such instruction should include an explanation of the detrimental effect that delays or the failure to report has on the security provided.

**Status.** Resolved – open.

**Summary of EOUSA Response.** EOUSA concurred with this recommendation and stated that it will notify the OIG when the *U.S. Attorneys' Manual* has been formally amended. In the interim, EOUSA issued a memorandum to all U.S. Attorneys reminding them that it is incumbent upon each USAO employee to notify the District Office Security Manager of all threats. The memorandum notes that threat reports play a critical role in helping the USMS assess the pattern and context of future threats. EOUSA provided the OIG with a copy of that memorandum under separate cover.

**OIG Analysis.** The actions planned by EOUSA are responsive to our recommendation. Please provide the OIG with a copy of the final, approved *U.S. Attorneys' Manual* amendments or a status report regarding the policy amendments by March 1, 2010.

**Recommendation 10.** EOUSA provide, in consultation with the USMS, sufficient training to EOUSA and USAO staff assigned threat response duties.

**Status.** Resolved – open.

**Summary of EOUSA Response.** EOUSA concurred with this recommendation and plans to consult with the USMS on the training curriculum.

**OIG Analysis.** Although EOUSA concurred with the recommendation, it did not provide any details regarding its training plans. Please provide the OIG with a timeline for implementation of revised training, information on who will be trained and how the training will be delivered, and a copy of the proposed training curriculum or a status report regarding the plans by March 1, 2010.

**Recommendation 11.** The USMS and EOUSA sign a memorandum of understanding that defines their roles and responsibilities in protecting U.S. Attorneys and AUSAs who receive threats.

**Status.** Resolved – open.

**Summary of EOUSA Response.** EOUSA concurred with the recommendation. EOUSA will consult with the USMS to produce a memorandum of understanding that defines the roles and responsibilities of EOUSA and the USMS when a threat is received by a USAO employee.

**OIG Analysis.** The actions planned by EOUSA are responsive to our recommendation. Please provide the OIG with a copy of the memorandum of understanding that describes the roles and responsibilities of EOUSA, USAOs, USMS headquarters, and USMS district offices by March 1, 2010.

**Recommendation 12.** EOUSA provide guidance and periodic reminders to USAOs of the requirement to submit Urgent Reports immediately when a U.S. Attorney or AUSA is threatened.

**Status.** Resolved – open.

**Summary of EOUSA Response.** EOUSA concurs with this recommendation. EOUSA issued a memorandum to all U.S. Attorneys, First Assistant U.S. Attorneys, District Office Security Managers, and Criminal Chiefs to remind all USAO employees to notify their District Office Security Manager and office management when a threat is received.

**OIG Analysis.** EOUSA issued a memorandum to all USAOs that is responsive to the intent of this recommendation. The memorandum reiterates the requirement in the *U.S. Attorneys' Manual* to immediately report to EOUSA via Urgent Report any threat to USAO personnel. However, we believe that periodic reminders by EOUSA of the reporting requirement should still be made to the USAOs. Please provide the OIG with a description, by March 1, 2010, of how often EOUSA intends to send reminders to all U.S. Attorneys, First Assistant U.S. Attorneys, District Office Security Managers, and Criminal Chiefs to remind all USAO employees to notify their District Office Security Manager and office management when a threat is received. Also, please provide the OIG with a copy of the next reminder when issued.

**Recommendation 13.** EOUSA revise the Urgent Report template so that it includes a requirement to provide at least the following information:

- name and position of targeted employee;
- name and location of the person making the threat, if known;

- date the threat was made, or date the target was made aware of the threat;
- date the District Office Security Manager was informed of the threat;
- date the USMS and FBI were notified; and
- date the USAO submitted the Urgent Report to EOUSA.

**Status.** Resolved – open.

**Summary of EOUSA Response.** EOUSA concurred with this recommendation and stated that it has made available to all USAOs a new threat reporting form covering the information in our recommendation. EOUSA is also developing a web-based Urgent Report system intended to facilitate timely and complete threat reporting that it hopes to pilot in the second quarter of 2010.

**OIG Analysis.** EOUSA concurred with the recommendation and provided a new threat reporting form to the USAOs that included the information in the recommendation. Please provide to us by March 1, 2010, the system requirements documents for the web-based Urgent Report system (specifically the section that includes the above elements as functional requirements for completion of the Urgent Report form), and a copy of the instructions to the USAOs for reporting threats using the system.

**Recommendation 14.** EOUSA establish guidance to require the District Office Security Managers to send updated information via Urgent Reports at regular intervals to inform EOUSA of the status of USAO, USMS, and FBI actions to protect the threatened AUSA.

**Status.** Resolved – open.

**Summary of EOUSA Response.** EOUSA concurred with this recommendation. EOUSA has issued a memorandum to all U.S. Attorneys to remind each office of the requirement to send updated information to EOUSA. EOUSA is also developing a web-based Urgent Report system intended to facilitate greater and more complete follow-up reporting from the districts.


**OIG Analysis.** Although EOUSA concurred with the recommendation, it has not established guidance that requires District Office Security Managers to send updated information via Urgent Reports to inform EOUSA of the status of actions taken to protect threatened USAO employees. The memorandum does not establish a requirement to send this

updated information and is not equivalent to amending current policy. Please provide us with a copy of the amended guidance that includes the requirement to provide updated information to EOUSA by March 1, 2010.

# Exhibit 24



[Home](#)   [About the Court](#)   [Attorneys](#)   [News Media](#)   [Employment](#)

[Electronic Filing - ECF](#)  
[Decisions](#)  
[Calendar](#)  
[Case Information](#)  
[FAQs, Forms and Instructions](#)  
[Rules](#)  
[Audio Recordings](#)  
[RSS Feeds](#) 

[Clerk's Office](#)  
[Mediation](#)  
[Appellate Commissioner](#)



#### Cases of Interest

(01/04/10) Perry v. Schwarzenegger, No. 09-17241, 09-17551 - All pleadings  
 (12/22/09) In the matter of Karen Golinski, No. 09-80173 - Order  
 (11/19/09) In the matter of Karen Golinski, No. 09-80173 - Order (2)  
 (11/19/09) In the matter of Karen Golinski, No. 09-80173 - Order (1)  
 (11/18/09) In the Matter of Brad Levenson, No. 09-80172 - Order  
 (11/10/09) In Re Gerald R. Smith, No. 09-80163 - Order For Publication  
 (11/05/09) USA v Hinkson, No. 05-30303 - Opinion  
 (10/22/09) Doe v Reed, No. 09-35818 - Opinion  
 (10/15/09) Doe v Reed, No. 09-35818 - Order

**Welcome** to the new website for the United States Court of Appeals for the Ninth Circuit. [more >>](#)

- Chief Judge Alex Kozinski



#### Announcements

(12/21/09) Notice and Opportunity for Comment on Rules... **NEW**  
 (12/17/09) Ninth Circuit to Allow Cameras in District Courts **NEW**  
 (12/14/09) IMPORTANT HOLIDAY NOTICE **NEW**  
 (12/07/09) Circuit Judge McKeown Recognized for Immigration... **NEW**  
 (12/02/09) Effective Saturday 12 December 2009, Appellate...  
 (12/01/09) Revisions to the Federal Rules of Appellate...

[Site Map](#) | [Intranet \(Judiciary Only\)](#) | [Seminar Disclosures](#) | [Judicial Misconduct](#) | [Suggestions](#)





## UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

Post Office Box 193939  
San Francisco, CA 94119-3939

### OPPORTUNITY FOR COMMENT - RULES GOVERNING JUDICIAL MISCONDUCT COMPLAINTS

The provisions noted below are potential additions to the existing procedures governing judicial misconduct complaints. Public comment on the supplementary language is invited. Responses are due on or before January 22, 2010 and should be directed to [Molly\\_Dwyer@ca9.uscourts.gov](mailto:Molly_Dwyer@ca9.uscourts.gov).

**Proposed Local Rule 6.1(b): Page Limit.** The statement of facts must not be longer than five pages (five sides), or 1,200 words, whichever is less. The complaint must be submitted on standard 8.5x11 size paper. A complainant may petition the Chief Judge for permission to submit additional pages if extraordinary circumstances exist.

**Proposed Local Rule 6.1(a): Name of Subject Judge.** Complainant must use the form appended to these rules. If complainant fails to identify the subject judge(s) on the first page of the form, the complaint will be returned to complainant with a request to do so.

**Proposed Local Rule 6.1(e): Number of Copies.** If the complaint is about a single judge, the complainant must file five copies of (1) the complaint form, (2) the statement of facts, and (3) any documents submitted. If the complaint is about more than one judge, one extra copy must be filed for each additional judge.

**Proposed Local Rule 18.1(b): Number of Copies.** The complainant must file an original and fifteen copies of the petition for review, along with ten copies of the original complaint.

January 8, 2010

Andrew P. Pugno  
LAW OFFICES OF ANDREW P.  
PUGNO  
101 Parkshore Dr., Ste. 100  
Folsom, CA 95630  
(916) 608-3065

Respectfully Submitted,

s/Michael W. Kirk

Charles J. Cooper  
Michael W. Kirk  
Jesse Panuccio  
COOPER & KIRK PLLC  
1523 New Hampshire Avenue, NW  
Washington, DC 20036  
202-220-9600

Brian W. Raum  
James A. Campbell  
ALLIANCE DEFENSE FUND  
15100 N. 90th St.  
Scottsdale, AZ 85260  
(480) 444-0020

*Counsel for Petitioners*

## DECLARATION OF SERVICE

I hereby certify that on the 8th day of January, 2010, I caused to be served on the following counsel a true and correct copy of the foregoing via FedEx Express:

Kenneth C. Mennemeier  
Andrew W. Stroud  
MENNEMEIER, GLASSMAN &  
STROUD LLP  
980 9th Street, Suite 1700  
Sacramento, CA 95814-2736  
[kcm@mgsllaw.com](mailto:kcm@mgsllaw.com)  
[gosling@mgsllaw.com](mailto:gosling@mgsllaw.com)  
[aknight@mgsllaw.com](mailto:aknight@mgsllaw.com)  
[stroud@mgsllaw.com](mailto:stroud@mgsllaw.com)  
[lbailey@mgsllaw.com](mailto:lbailey@mgsllaw.com)

*Attorneys for the Administration Defendants*

Dennis J. Herrera  
Therese M. Stewart  
OFFICE OF THE CITY ATTORNEY  
City Hall, Room 234  
One Dr. Carlton B. Goodlett Place  
San Francisco, California 94102-4682  
[therese.stewart@sfgov.org](mailto:therese.stewart@sfgov.org)  
[erin.bernstein@sfgov.org](mailto:erin.bernstein@sfgov.org)  
[vince.chhabria@sfgov.org](mailto:vince.chhabria@sfgov.org)  
[danny.chou@sfgov.org](mailto:danny.chou@sfgov.org)  
[ronald.flynn@sfgov.org](mailto:ronald.flynn@sfgov.org)  
[mollie.lee@sfgov.org](mailto:mollie.lee@sfgov.org)  
[Christine.van.aken@sfgov.org](mailto:Christine.van.aken@sfgov.org)  
[catheryn.daly@sfgov.org](mailto:catheryn.daly@sfgov.org)

*Attorneys for Plaintiff-Intervenor City and County of San Francisco*

Gordon Burns  
Tamar Pachter  
OFFICE OF THE ATTORNEY  
GENERAL  
1300 I Street, Suite 125  
P.O Box. 944255  
Sacramento, CA 94244-2550  
[Gordon.Burns@doj.ca.gov](mailto:Gordon.Burns@doj.ca.gov)  
[Tamar.Pachter@doj.ca.gov](mailto:Tamar.Pachter@doj.ca.gov)

*Attorneys for Defendant Attorney General  
Edmund G. Brown, Jr.*

Elizabeth M. Cortez  
Judy W. Whitehurst  
THE OFFICE OF CITY COUNSEL  
648 Kenneth Hahn Hall of Administration  
500 West Temple Street  
Los Angeles, CA 90012-2713  
[jwhitehurst@counsel.lacounty.gov](mailto:jwhitehurst@counsel.lacounty.gov)

*Attorneys for Defendant Dean C. Logan  
Registrar-Recorder/County Clerk,  
County  
of Los Angeles*

Richard E Winnie  
Brian E. Washington  
Claude F. Kolm  
Manuel F. Martinez  
THE OFFICE OF CITY COUNSEL  
1221 Oak Street, Suite 450  
Oakland, California 94612  
[Brian.washington@acgov.org](mailto:Brian.washington@acgov.org)  
[Claude.kolm@acgov.org](mailto:Claude.kolm@acgov.org)  
[Lindsey.stern@acgov.org](mailto:Lindsey.stern@acgov.org)  
[Judith.martinez@acgov.org](mailto:Judith.martinez@acgov.org)

*Attorneys for Defendant Patrick  
O'Connell  
Clerk Recorder of the County of Alameda*

Ted Olson  
Matthew McGill  
Amir Tayrani  
GIBSON, DUNN & CRUTCHER  
LLP  
1050 Connecticut Avenue, N.W.  
Washington, DC 20036-5306  
T: (202) 955-8500  
F: (202) 467-0539  
[TOlson@gibsondunn.com](mailto:TOlson@gibsondunn.com)  
[MMcGill@gibsondunn.com](mailto:MMcGill@gibsondunn.com)  
[ATayrani@gibsondunn.com](mailto:ATayrani@gibsondunn.com)

Theodore Boustrous, Jr.  
Christopher Dusseault  
Theane Kapur  
GIBSON, DUNN & CRUTCHER  
LLP  
333 South Grand Avenue  
Los Angeles, CA 90072-1512  
T: (213) 229-7000  
F: (213) 229-7520  
[TBoutrous@gibsondunn.com](mailto:TBoutrous@gibsondunn.com)  
[CDusseault@gibsondunn.com](mailto:CDusseault@gibsondunn.com)  
[TKapur@gibsondunn.com](mailto:TKapur@gibsondunn.com)  
[SMalzahn@gibsondunn.com](mailto:SMalzahn@gibsondunn.com)

Ethan Dettmer  
Enrique Monagas  
GIBSON, DUNN & CRUTCHER  
LLP  
555 Mission Street, Suite 3000  
San Francisco, CA 94105  
T: (415) 393-8200  
F: (415) 393-8306  
[EDettmer@gibsondunn.com](mailto:EDettmer@gibsondunn.com)

[SPiepmeier@gibsondunn.com](mailto:SPiepmeier@gibsondunn.com)  
[EMonagas@gibsondunn.com](mailto:EMonagas@gibsondunn.com)  
[RJustice@gibsondunn.com](mailto:RJustice@gibsondunn.com)  
[MJanky@gibsondunn.com](mailto:MJanky@gibsondunn.com)

Theodore Uno  
BOIES, SCHILLER & FLEXNER  
LLP  
1999 Harrison Street, Suite 900  
Oakland, CA 94612  
T: (510) 874-1000  
F: (510) 874-1460  
[jgoldman@bsflp.com](mailto:jgoldman@bsflp.com)  
[tuno@bsflp.com](mailto:tuno@bsflp.com)  
[brichardson@bsflp.com](mailto:brichardson@bsflp.com)  
[rbettan@bsflp.com](mailto:rbettan@bsflp.com)  
[jischiller@bsflp.com](mailto:jischiller@bsflp.com)

*Attorneys for Plaintiff Kristin M.  
Perry*

I hereby certify that on the 8th day of January, 2010, I caused to be served on the following counsel a true and correct copy of the foregoing via United States Postal Service express mail overnight delivery:

Terry L. Thompson  
LAW OFFICE OF TERRY L. THOMPSON  
P.O. Box 1346  
Alamo, CA 94507  
T: (925) 855-1507  
F: (925) 820-6035  
[tl\\_thompson@earthlink.net](mailto:tl_thompson@earthlink.net)

*Attorney for Defendant-Intervenor Hak-Shing William Tam*

s/Jesse Panuccio  
Jesse Panuccio