

~~TOP SECRET//COMINT//ORCON,NOFORN~~

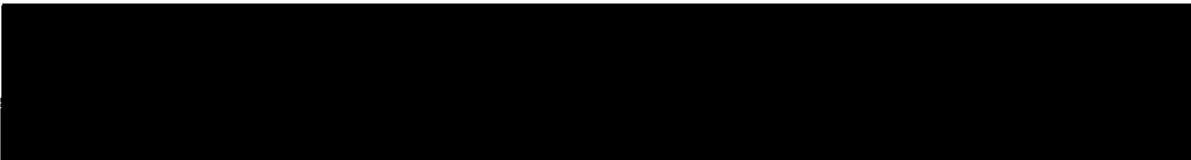
U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT ~~269 MAR 17 AM 11:40~~

WASHINGTON, D.C.

CLERK OF COURT



**GOVERNMENT'S SUPPLEMENT TO ITS RESPONSE TO THE COURT'S ORDER
OF JANUARY 16, 2009**

THE UNITED STATES OF AMERICA, through the undersigned Department of Justice attorney, respectfully submits the attached supplement to the government's January 26, 2009, response to the Court's Order of January 16, 2009, concerning [REDACTED]

[REDACTED] and the targeting and minimization procedures submitted therewith. The Government may seek to augment and/or modify the information provided in its January 26, 2009, response, and this supplement thereto, as appropriate during any hearing that the Court may hold in the above-captioned matter. (S//OC,NF)

Respectfully submitted
(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Deputy Unit Chief
National Security Division
United States Department of Justice

~~TOP SECRET//COMINT//ORCON,NOFORN~~

Classified by:

Matthew G. Olsen, Deputy Assistant Attorney General, NSD, DOJ

Reason:

1.4(c)

Declassify on:

17 March 2034

(U) Executive Summary

~~(TS//SI//NF)~~ This report for the Foreign Intelligence Surveillance Court describes a circumstance where the National Security Agency (“NSA” or “Agency”) acquires more communications than intended (“overcollection”) during signals intelligence activities authorized pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended, and the steps NSA has taken to correct such incidents of overcollection. In order to fully describe the problem and NSA’s corrective measures, this report also describes relevant aspects of the Agency’s collection methods, technical architecture, and the equipment, systems, and procedures NSA employs to identify and correct instances of overcollection. NSA is confident that the corrective measures NSA has designed, tested, and fielded to correct the overcollection problem form a reasoned and appropriate response to past instances of overcollection. There remains one known instance of overcollection for which NSA is developing a corrective measure as discussed herein. These corrective measures are subject to continuing improvement and NSA personnel also continue to monitor the Agency’s collection activities for signs of overcollection. Although no corrective measure is perfect, NSA has taken significant steps to mitigate the possibility of any future overcollection and to ensure that the detection mechanisms in place to identify overcollection will allow NSA to respond quickly if and when it does occur.

I. ~~(TS//SI//REL USA, FVEY)~~ Description of NSA’s Upstream Collection

~~(TS//SI//REL)~~ Pursuant to the signals intelligence authority provided to the National Security Agency (“NSA” or “Agency”) by Executive Order 12333, as amended; National Security Council Intelligence Directive No. 6; the NSA Act of 1959, as amended; and other applicable law and policy direction, [REDACTED] NSA has developed and evolved techniques for selecting and processing Internet communications for the purpose of obtaining foreign intelligence. [REDACTED]

[REDACTED] NSA uses [REDACTED] collection techniques to acquire communications whose acquisition is regulated by the FISA, to include collecting communications pursuant to certifications executed in accordance with Section 702 of the FISA Amendments Act of 2008 (“FAA”).¹ [REDACTED]

~~(TS//SI//NF)~~ NSA’s FAA collection of Internet communications (e.g., e-mail communications to, from, or about a targeted e-mail selector) is accomplished [REDACTED]

¹ (U) NSA personnel frequently refer to the Agency’s non-FISA collection activity as “12333 collection.” In contrast, NSA personnel frequently refer to collection accomplished pursuant to Section 702 of the FAA as “FAA collection.”

~~Derived From: NSA/CSSM 1-52~~

~~Dated: 20070108~~

~~Declassify On: 20320108~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

Internet Service Providers ("ISPs") provide information contained in targeted accounts under the ISP's control; [REDACTED]

[REDACTED] collection listed above are referred to as "Upstream Collection" in the government's response to the Court's January 16, 2009 Order concerning DNI/ [REDACTED] ("Government's Response").

~~(TS//SI//NF)~~ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

² (U) Examples of [REDACTED]

³ (U) As used in this context, [REDACTED]

⁴ (TS//SI//NF) [REDACTED]

~~TOP SECRET//COMINT//NOFORN//20320108~~

-(TS//SI//NF) Not only does [REDACTED] compensate for [REDACTED]

[REDACTED] is uniquely capable of acquiring certain types of targeted communications containing valuable foreign intelligence information

[REDACTED] For example, [REDACTED]

[REDACTED] Similarly, it allows NSA to [REDACTED]

In both of these examples, the communications acquired through [REDACTED] may help NSA ascertain [REDACTED] previously unknown individuals who may also possess and/or communicate valuable foreign intelligence information. Additionally, [REDACTED]

II.-(TS//SI//NF) Description of

-(TS//SI//NF)-

-TS//SI//NF

5 ~~(TS/SU/NE)~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

[REDACTED]

III. ~~(TS//SI//NF)~~ Overcollection and the Evolution of NSA's [REDACTED]

Systems

~~(TS//SI//NF)~~ Any collection technique that NSA employs may result in the inadvertent collection of communications NSA did not intend to acquire.⁶ As described previously, the [REDACTED] provides unique foreign intelligence information. However, it also comes with the potential for producing overcollection, including [REDACTED] Overcollection ([REDACTED]). [REDACTED] occurs when, while collecting communications [REDACTED] the Agency also inadvertently acquires other communications that [REDACTED]

~~(TS//SI//NF)~~ [REDACTED]

A. ~~(TS//SI//NF)~~ [REDACTED]

~~(TS//SI//NF)~~ [REDACTED]

⁶ ~~(S//SI//REL)~~ NSA handles any inadvertent collection of US person information in accordance with the Court-approved minimization procedures corresponding to the specific FAA certification under which NSA acquired the information.

⁷ ~~(TS//SI//REL)~~ [REDACTED]

~~TOP SECRET//COMINT//NOFORN//20320108~~

-TS//SI//NF-

B. - (TS//SI//NF)

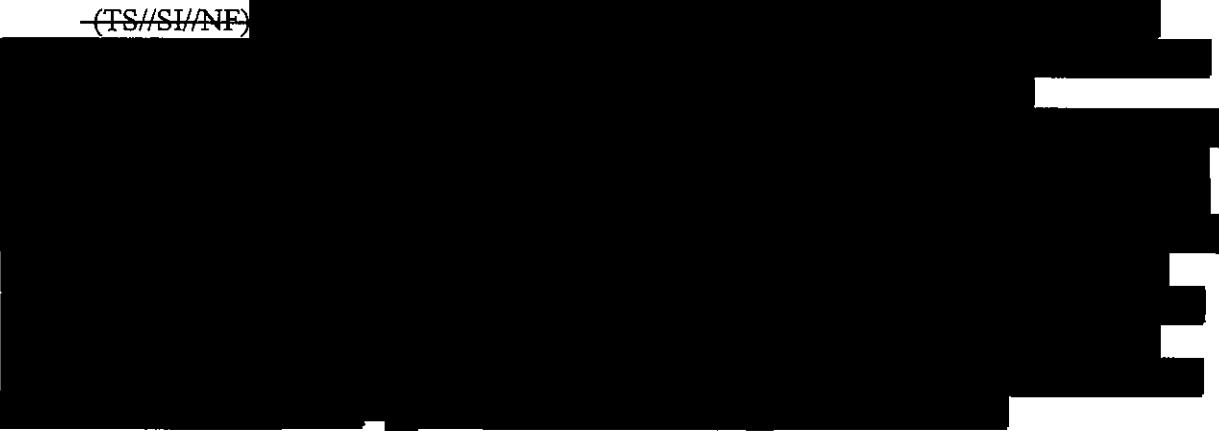
~~(TS//SI//NF)~~

⁸ (TS//SI//NF)

9 (TS/SL/NF)

10 (TS/SI/NF)

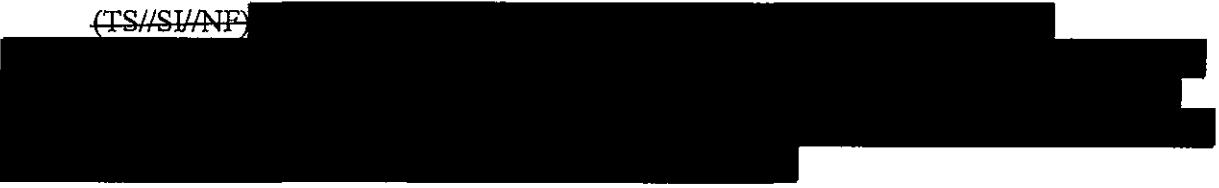
~~-(TS//SI//NF)~~



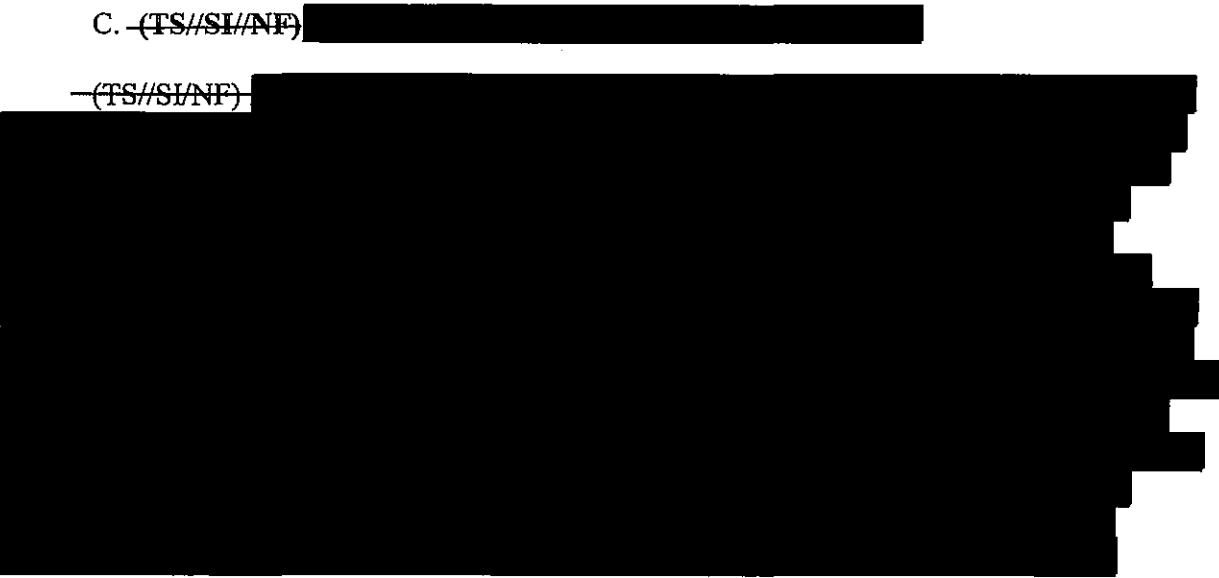
~~-(TS//SI//NF)~~



~~-(TS//SI//NF)~~



C. ~~-(TS//SI//NF)~~



¹¹ ~~(TS//SI//NF)~~ NSA technical personnel evaluated approximately [REDACTED] files during this week long test, and approximately [REDACTED] additional files in subsequent testing.

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~-(TS//SI//NF)~~

D. ~~(TS//SI//NF)~~

~~-(TS//SI//NF)~~

IV. (TS//SI//NF) Review of Overcollection Incidents

(TS//SI//NF) In recent notices the Department of Justice filed with the Court pursuant to Rule 10(c) of the Rules of Procedure for the Foreign Intelligence Surveillance Court, the Government described [REDACTED] overcollection incidents arising from NSA's use of [REDACTED]

¹² [REDACTED] of these [REDACTED] incidents were examples of [REDACTED] O.

12 (TS/SL/NE)

Table 1 briefly summarizes each incident.

[REDACTED]

(TS//SI//NF) A summary of all [REDACTED] recent overcollection incidents is provided in Table 1. The [REDACTED] additional incidents referenced on page 15 of the Government's Response¹⁴ were also incidents of [REDACTED] O. Specifically, in [REDACTED] 2007 while conducting foreign intelligence acquisition in accordance with the Protect America Act of 2007 ("PAA"), NSA discovered [REDACTED] O resulting from [REDACTED]

[REDACTED]

To be clear, NSA discovered this [REDACTED]
in [REDACTED] 2007 and took immediate steps to [REDACTED]
NSA has purged every file collected [REDACTED] during the time period [REDACTED]

[REDACTED]

(TS//SI//NF) The [REDACTED] overcollection (also discovered by NSA in [REDACTED] 2007) is described on page 15 of the Government's Response, and again here, as the [REDACTED]

[REDACTED] Specifically, in [REDACTED] 2007, during NSA's implementation of foreign intelligence acquisition authorized under the PAA, NSA implemented [REDACTED] at the request of the Agency's Office of Oversight and Compliance. [REDACTED]

¹³ (U//FOUO)

¹⁴ (TS//SI//NF) In addition to the overcollection incidents resulting from NSA's upstream collection techniques, there have been other isolated incidents involving 702 acquisitions of a substantially different nature. For example, as has been previously reported to the Court, there have been a few incidents in which the selectors of a United States person subject to traditional FISA coverage or a Section 704 order have been erroneously targeted under Section 702. Additionally, there have been other incidents involving the targeting or minimization procedures, including several selectors mistasked due to typographical errors in the targeting process and human errors that caused delays in the detasking of accounts where the user was known to be arriving in the United States. These latter incidents are reported to the Court in the Section 702(l) joint Department of Justice/Office of the Director of National Intelligence assessment and/or in the Section 707 Semiannual Report to Congress Concerning Acquisitions Under Section 702 of the FISA Amendments Act, a courtesy copy of which will be provided to the Court.

[REDACTED] In response, NSA purged every communication collected [REDACTED] during the relevant timeframe [REDACTED] 2007). NSA also [REDACTED] remedy for this problem by [REDACTED] 2007, [REDACTED] Subsequent testing revealed this remedy was successful, [REDACTED]

V. (TS//SI//NF) Additional Steps to Identify Overcollection

(TS//SI//NF) In addition to [REDACTED]

NSA continues to track and routinely monitor [REDACTED] looking for anomalies [REDACTED] that are indicative of [REDACTED] O.

(TS//SI//NF) NSA has also made analysts aware of the potential for these [REDACTED] O events and is providing instruction and training on how to recognize and report potential cases. Prior to being granted access to any FAA data, NSA analysts undergo formal training and competency testing on the FAA targeting and minimization procedures. This training is augmented by informal on-the-job training conducted by technical personnel as well as oversight personnel. The end result is that NSA analysts are trained to verify that the communications they are reviewing are, in fact, associated with the intended target and that the target remains a non-United States person located outside of the United States. Analysts have also been alerted to the possibility of overcollection of communications and have been provided hypothetical examples of what to look for when conducting post-collection reviews. In the event of possible overcollection, analysts are instructed to contact their organization's FAA Point of Contact who initiates an internal NSA review of a possible compliance incident. Samples of the data are then evaluated by technical personnel to confirm or refute that overcollection may have occurred. Confirmation of any occurrence of overcollection results in notification to NSA's Office of General Counsel which in turn reports these to the Department of Justice and the Office of the Director of National Intelligence in accordance with NSA's FAA Targeting Procedures. In addition, proper application of the minimization and targeting procedures that govern NSA's FAA collection also helps ensure that overcollection does not result in improper dissemination of information that may have been obtained through overcollection.

VI. ~~(TS//SI//NF)~~ NSA's Handling of Information Resulting from Overcollection

~~(TS//SI//NF)~~ Once an overcollection incident has been confirmed, NSA takes the required steps to isolate and purge all unminimized data from its repositories. Overcollected data can be purged from on-line databases using a variety of methods, all of which render it inaccessible in any new analyst queries. This may involve purging data that was appropriately acquired in addition to the data that was inadvertently acquired. For example, regarding the [REDACTED] incident, NSA purged all data collected as a result of targeting that selector during the entire timeframe of this incident. [REDACTED]

~~(TS//SI//NF)~~ Regarding dissemination, although the likelihood that any minimized FAA data resulting from overcollection would be disseminated in serialized product reporting is extremely small, in view of the fact that the inadvertent collection was unrelated to any targeted communications, NSA confirms that no such reporting occurred. In the case of the reported FAA overcollection incidents discussed here and in the Government's Response, NSA determined that no serialized product reports had been disseminated. This was accomplished by searching NSA's [REDACTED]

[REDACTED] If any information had been disseminated in serialized product, NSA would take the required steps to cancel/recall such reporting.

VII. ~~(TS//SI//NF)~~ The Five-Year Retention Period Established by NSA's Minimization Procedures is Reasonable Notwithstanding the Overcollection

~~(TS//SI//NF)~~ NSA submits, for the following reasons, that the five-year data retention period established by NSA's minimization procedures is reasonable notwithstanding the overcollection incidents described herein. As discussed above in detail, NSA has taken considerable steps to identify and purge overcollected communications acquired as a result of these incidents -- regardless of whether such communications contain information of or concerning United States persons -- and to prevent any future occurrences of [REDACTED]. Furthermore, the NSA minimization procedures work to dramatically reduce, if not eliminate, the impact of any incidental and inadvertent intrusions into the privacy of United States persons in the event that NSA retains any unidentified overcollected communications. Indeed, the likelihood that NSA analysts would even come across a previously unidentified overcollected communication of

¹⁵ ~~(TS//SI//NF)~~ [REDACTED]

~~TOP SECRET//COMINT//NOFORN//20320108~~

or concerning a United States person during the regular course of their duties is minimal. As noted above, the amount of overcollected data, relative to the overall amount of properly acquired data collected by the NSA pursuant to the FAA, is quite small.¹⁶ In addition, section 3(b)(5) of the NSA minimization procedures requires that all computer queries of collected communications stored in NSA data repositories "shall be limited to those selection terms reasonably likely to return foreign intelligence targets." Inasmuch as the overcollection described herein resulted in the inadvertent acquisition of communications wholly unrelated to targeted selectors used by properly targeted foreign intelligence targets, it is unlikely that NSA analysts, using appropriately tailored queries, would retrieve -- let alone analyze and disseminate -- any previously unidentified overcollected communication for review.¹⁷

(TS//SI//NF) Moreover, even in the unlikely event that an NSA analyst's query does retrieve an overcollected communication of or about a United States person, section 3(b)(1) of the NSA minimization procedures requires the destruction of that communication as soon as it is recognized. NSA analysts are being trained to identify overcollection incidents and promptly report them to oversight personnel so that appropriate measures -- including the destruction of all communications inadvertently acquired as a result of such incidents (regardless of whether they contain information of or concerning a United States person) -- can be taken.

(TS//SI//NF) In sum, NSA's minimization procedures operate to dramatically reduce, if not eliminate, the impact of any incidental and inadvertent intrusions into the privacy of United States persons that may result from NSA's retention of unidentified overcollected communications for the five-year period established by those procedures. Accordingly, NSA submits that this retention period is reasonable.

VIII. (U) Conclusion

(TS//SI//NF) As discussed above, NSA has developed new generation [REDACTED] and new generation [REDACTED] which greatly reduce the likelihood of overcollection or the extent to which it might occur. NSA has also developed [REDACTED] as an additional layer of protection against [REDACTED] O incidents. NSA has further educated and sensitized its work force to the problem of overcollection, how to identify possible instances of it and how to report it when it is identified. It is important to note that NSA has not been able to identify any circumstance where an overcollection incident resulted in the dissemination of overcollected information outside of the NSA SIGINT production chain (analysts and others authorized with access to unminimized FAA data).

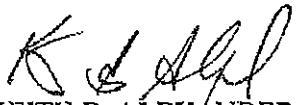
¹⁶ (TS//SI//NF) Given the efficacy of the measures NSA has taken to date in response to the incidents described herein, NSA expects that any future occurrences of [REDACTED] O that may occur would involve even smaller volumes of overcollected communications.

¹⁷ (TS//SI//NF) Moreover, analysts' queries are routinely audited by trained personnel in the various SIGINT product lines and superaudited by NSA oversight and compliance personnel to ensure that all such queries are consistent with NSA's minimization procedures.

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~TOP SECRET//COMINT//NOFORN//20320108~~

~~(TS//SI//NF)~~ Except in the [REDACTED] NSA has been able to identify the causes of the incidents of overcollection and has taken extensive and multi-layered steps to prevent similar incidents in the future. NSA has purged all of the data it has identified as overcollection. There is no guarantee that future [REDACTED] problems will not occur, or that future [REDACTED] changes, which NSA may not have anticipated, and which [REDACTED] Nonetheless, NSA has reason to be confident that [REDACTED] work as designed. In sum, NSA has taken significant steps to mitigate the possibility of any future overcollection and to ensure that the detection mechanisms in place to identify overcollection will allow NSA to respond quickly if and when it does occur.



KEITH B. ALEXANDER
Lieutenant General, U.S. Army
Director, National Security Agency

~~TOP SECRET//COMINT//NOFORN//20320108~~

Table 1. Summary of Overcollection Incidents

Category	Description	Count
1	Incident 1	1
2	Incident 2	1
3	Incident 3	1
4	Incident 4	1
5	Incident 5	1
6	Incident 6	1
7	Incident 7	1
8	Incident 8	1
9	Incident 9	1
10	Incident 10	1
11	Incident 11	1
12	Incident 12	1
13	Incident 13	1
14	Incident 14	1
15	Incident 15	1
16	Incident 16	1
17	Incident 17	1
18	Incident 18	1
19	Incident 19	1
20	Incident 20	1
21	Incident 21	1
22	Incident 22	1
23	Incident 23	1
24	Incident 24	1
25	Incident 25	1
26	Incident 26	1
27	Incident 27	1
28	Incident 28	1
29	Incident 29	1
30	Incident 30	1
31	Incident 31	1
32	Incident 32	1
33	Incident 33	1
34	Incident 34	1
35	Incident 35	1
36	Incident 36	1
37	Incident 37	1
38	Incident 38	1
39	Incident 39	1
40	Incident 40	1
41	Incident 41	1
42	Incident 42	1
43	Incident 43	1
44	Incident 44	1
45	Incident 45	1
46	Incident 46	1
47	Incident 47	1
48	Incident 48	1
49	Incident 49	1
50	Incident 50	1
51	Incident 51	1
52	Incident 52	1
53	Incident 53	1
54	Incident 54	1
55	Incident 55	1
56	Incident 56	1
57	Incident 57	1
58	Incident 58	1
59	Incident 59	1
60	Incident 60	1
61	Incident 61	1
62	Incident 62	1
63	Incident 63	1
64	Incident 64	1
65	Incident 65	1
66	Incident 66	1
67	Incident 67	1
68	Incident 68	1
69	Incident 69	1
70	Incident 70	1
71	Incident 71	1
72	Incident 72	1
73	Incident 73	1
74	Incident 74	1
75	Incident 75	1
76	Incident 76	1
77	Incident 77	1
78	Incident 78	1
79	Incident 79	1
80	Incident 80	1
81	Incident 81	1
82	Incident 82	1
83	Incident 83	1
84	Incident 84	1
85	Incident 85	1
86	Incident 86	1
87	Incident 87	1
88	Incident 88	1
89	Incident 89	1
90	Incident 90	1
91	Incident 91	1
92	Incident 92	1
93	Incident 93	1
94	Incident 94	1
95	Incident 95	1
96	Incident 96	1
97	Incident 97	1
98	Incident 98	1
99	Incident 99	1
100	Incident 100	1
101	Incident 101	1
102	Incident 102	1
103	Incident 103	1
104	Incident 104	1
105	Incident 105	1
106	Incident 106	1
107	Incident 107	1
108	Incident 108	1
109	Incident 109	1
110	Incident 110	1
111	Incident 111	1
112	Incident 112	1
113	Incident 113	1
114	Incident 114	1
115	Incident 115	1
116	Incident 116	1
117	Incident 117	1
118	Incident 118	1
119	Incident 119	1
120	Incident 120	1
121	Incident 121	1
122	Incident 122	1
123	Incident 123	1
124	Incident 124	1
125	Incident 125	1
126	Incident 126	1
127	Incident 127	1
128	Incident 128	1
129	Incident 129	1
130	Incident 130	1
131	Incident 131	1
132	Incident 132	1
133	Incident 133	1
134	Incident 134	1
135	Incident 135	1
136	Incident 136	1
137	Incident 137	1
138	Incident 138	1
139	Incident 139	1
140	Incident 140	1
141	Incident 141	1
142	Incident 142	1
143	Incident 143	1
144	Incident 144	1
145	Incident 145	1
146	Incident 146	1
147	Incident 147	1
148	Incident 148	1
149	Incident 149	1
150	Incident 150	1
151	Incident 151	1
152	Incident 152	1
153	Incident 153	1
154	Incident 154	1
155	Incident 155	1
156	Incident 156	1
157	Incident 157	1
158	Incident 158	1
159	Incident 159	1
160	Incident 160	1
161	Incident 161	1
162	Incident 162	1
163	Incident 163	1
164	Incident 164	1
165	Incident 165	1
166	Incident 166	1
167	Incident 167	1
168	Incident 168	1
169	Incident 169	1
170	Incident 170	1
171	Incident 171	1
172	Incident 172	1
173	Incident 173	1
174	Incident 174	1
175	Incident 175	1
176	Incident 176	1
177	Incident 177	1
178	Incident 178	1
179	Incident 179	1
180	Incident 180	1
181	Incident 181	1
182	Incident 182	1
183	Incident 183	1
184	Incident 184	1
185	Incident 185	1
186	Incident 186	1
187	Incident 187	1
188	Incident 188	1
189	Incident 189	1
190	Incident 190	1
191	Incident 191	1
192	Incident 192	1
193	Incident 193	1
194	Incident 194	1
195	Incident 195	1
196	Incident 196	1
197	Incident 197	1
198	Incident 198	1
199	Incident 199	1
200	Incident 200	1
201	Incident 201	1
202	Incident 202	1
203	Incident 203	1
204	Incident 204	1
205	Incident 205	1
206	Incident 206	1
207	Incident 207	1
208	Incident 208	1
209	Incident 209	1
210	Incident 210	1
211	Incident 211	1
212	Incident 212	1
213	Incident 213	1
214	Incident 214	1
215	Incident 215	1
216	Incident 216	1
217	Incident 217	1
218	Incident 218	1
219	Incident 219	1
220	Incident 220	1
221	Incident 221	1
222	Incident 222	1
223	Incident 223	1
224	Incident 224	1
225	Incident 225	1
226	Incident 226	1
227	Incident 227	1
228	Incident 228	1
229	Incident 229	1
230	Incident 230	1
231	Incident 231	1
232	Incident 232	1
233	Incident 233	1
234	Incident 234	1
235	Incident 235	1
236	Incident 236	1
237	Incident 237	1
238	Incident 238	1
239	Incident 239	1
240	Incident 240	1
241	Incident 241	1
242	Incident 242	1
243	Incident 243	1
244	Incident 244	1
245	Incident 245	1
246	Incident 246	1
247	Incident 247	1
248	Incident 248	1
249	Incident 249	1
250	Incident 250	1
251	Incident 251	1
252	Incident 252	1
253	Incident 253	1
254	Incident 254	1
255	Incident 255	1
256	Incident 256	1
257	Incident 257	1
258	Incident 258	1
259	Incident 259	1
260	Incident 260	1
261	Incident 261	1
262	Incident 262	1
263	Incident 263	1
264	Incident 264	1
265	Incident 265	1
266	Incident 266	1
267	Incident 267	1
268	Incident 268	1
269	Incident 269	1
270	Incident 270	1
271	Incident 271	1
272	Incident 272	1
273	Incident 273	1
274	Incident 274	1
275	Incident 275	1
276	Incident 276	1
277	Incident 277	1
278	Incident 278	1
279	Incident 279	1
280	Incident 280	1
281	Incident 281	1
282	Incident 282	1
283	Incident 283	1
284	Incident 284	1
285	Incident 285	1
286	Incident 286	1
287	Incident 287	1
288	Incident 288	1
289	Incident 289	1
290	Incident 290	1
291	Incident 291	1
292	Incident 292	1
293	Incident 293	1
294	Incident 294	1
295	Incident 295	1
296	Incident 296	1
297	Incident 297	1
298	Incident 298	1
299	Incident 299	1
300	Incident 300	1
301	Incident 301	1
302	Incident 302	1
303	Incident 303	1
304	Incident 304	1
305	Incident 305	1
306	Incident 306	1
307	Incident 307	1
308	Incident 308	1
309	Incident 309	1
310	Incident 310	1
311	Incident 311	1
312	Incident 312	1
313	Incident 313	1
314	Incident 314	1
315	Incident 315	1
316	Incident 316	1
317	Incident 317	1
318	Incident 318	1
319	Incident 319	1
320	Incident 320	1
321	Incident 321	1
322	Incident 322	1
323	Incident 323	1
324	Incident 324	1
325	Incident 325	1
326	Incident 326	1
327	Incident 327	1
328	Incident 328	1
329	Incident 329	1
330	Incident 330	1
331	Incident 331	1
332	Incident 332	1
333	Incident 333	1
334	Incident 334	1
335	Incident 335	1
336	Incident 336	1
337	Incident 337	1
338	Incident 338	1
339	Incident 339	1
340	Incident 340	1
341	Incident 341	1
342	Incident 342	1
343	Incident 343	1
344	Incident 344	1
345	Incident 345	1
346	Incident 346	1
347	Incident 347	1
348	Incident 348	1
349	Incident 349	1
350	Incident 350	1
351	Incident 351	1
352	Incident 352	1
353	Incident 353	1
354	Incident 354	1
355	Incident 355	1
356	Incident 356	1
357	Incident 357	1
358	Incident 358	1
359	Incident 359	1
360	Incident 360	1
361	Incident 361	1
362	Incident 362	1
363	Incident 363	1
364	Incident 364	1
365	Incident 365	1
366	Incident 366	1
367	Incident 367	1
368	Incident 368	1
369	Incident 369	1
370	Incident 370	1
371	Incident 371	1
372	Incident 372	1
373	Incident 373	1
374	Incident 374	1
375	Incident 375	1
376	Incident 376	1
377	Incident 377	1
378	Incident 378	1
379	Incident 379	1
380	Incident 380	1
381	Incident 381	1
382	Incident 382	1
383	Incident 383	1
384	Incident 384	1
385	Incident 385	1

Table 2: [REDACTED]
January 16, 2009 [REDACTED]

