

**SECRET**

FOIA review completed on 4 January 2018. Portions of this document no longer meet the classification standards of E.O. 13526, Section 1.4. As such, I am downgrading specific portion-marked paragraphs as "UNCLASSIFIED." Partial classification downgrade executed by:  
  
DANIEL L. KARBLER  
Major General, U.S. Army  
Chief of Staff  
U.S. Strategic Command

1  
2  
3  
4  
5  
6  
7  
8

**HEADQUARTERS**  
**UNITED STATES**

**STRATEGIC COMMAND**



9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23

**CDRUSSTRATCOM CONPLAN 8039-08 (U)**

~~Classified By: Multiple Sources~~  
~~Reason: 1.4 (a), (e), and (g)~~  
~~Declassify On: Feb 2032~~

**SECRET**

**SECRET**

24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45

(INTENTIONALLY BLANK)

**SECRET**

**SECRET**

46 HEADQUARTERS, U.S. STRATEGIC COMMAND  
47 OFFUTT AIR FORCE BASE NE 68113-6500  
48 28 February 2008  
49

50 USSTRATCOM CONPLAN 8039-08 (U)

51 Table of Contents (U)

52

<b>CONTENTS</b>	<b>PAGE</b>
Letter of Transmittal	v
Security Instructions	vii
Classification Guidance	ix
Plan Summary	xi
Terms of Reference	xix
Base Plan	1
Situation	6
Mission Statement	14
Execution	15
Administration & Logistics	65
Command & Control	66
ANNEX A – Task Organization	A-1
ANNEX B – Intelligence	B-1
ANNEX C – Operations	C-1
ANNEX F – Public Affairs	F-1
ANNEX J – Command Relationships	J-1
ANNEX K – Command, Control, Communications & Computer Systems	K-1
ANNEX N – Space Operations	N-1
ANNEX S – Special Technical Operations	S-1
ANNEX V – Interagency Collaboration	V-1
ANNEX Y – Space Control Target Folders	Y-1
ANNEX Z - Distribution	Z-1

53

54

**SECRET**

**SECRET**

55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77

(INTENTIONALLY BLANK)

**SECRET**

**SECRET**

HEADQUARTERS, U.S. STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE NE 68113-6500  
28 February 2008

78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119

USSTRATCOM CONPLAN 8039-08 (U)

Letter of Transmittal (U)

SEE DISTRIBUTION (Annex Z)

1. (U) CDRUSSTRATCOM CONPLAN 8039-08, which provides for  
Cyberspace Operations, is attached.

2. (U) CONPLAN 8039-08 accomplishes the following:

(~~S~~//REL USA, AUS, GBR) Fulfills the (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(U) Establishes a common context providing linkages among operations  
in and through cyberspace and operations in all environments.

(U) Identifies threats and prioritizes planning efforts.

(U) (b)(1) Sec 1.7(e) it provides a methodology for  
(b)(1) Sec 1.7(e)

(U) Provides a framework for structuring pre-planned authorities to  
execute tasks that generate desired effects in support of national  
objectives.

3. (U) Elements of this plan were coordinated with Service Components,  
Functional Components, and supporting agencies during preparation.

4. (U) Upon approval, CDRUSSTRATCOM CONPLAN 8039-08 supersedes  
previous versions of CDRUSSTRATCOM CONPLAN 8039.

5. (U) File this letter in front of the plan.

FOR THE COMMANDER:

//signed//

MARK H. OWEN  
Brigadier General, USAF  
Director, Plans and Policy

**SECRET**

120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141

(INTENTIONALLY BLANK)

**SECRET**

**SECRET**

HEADQUARTERS, U.S. STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE NE 68113-6500  
28 February 2008

142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177

USSTRATCOM CONPLAN 8039-08 (U)  
Security Instructions & Record of Changes (U)

(U) Plan Title:

1. (U) The long title of this plan is CDRUSSTRATCOM CONPLAN 8039-08 CYBERSPACE OPERATIONS (U).
2. (U) The short title of this plan is CDRUSSTRATCOM CONPLAN 8039-08 (U).
3. (U) This document is classified SECRET//REL TO USA, AUS and GBR to protect information revealing operational plans of US military forces. CDRUSSTRATCOM CONPLAN 8039-08 must be disseminated only to those agencies and personnel whose official duties specifically require knowledge of the plan, including those required to develop supporting plans.
4. (U) This document contains information affecting the national defense of the United States within the meaning of the Espionage Laws, title 18, United States Code, sections 793 and 794. The transmission or revelation of information contained herein, in any manner, to an unauthorized person is prohibited by law.
5. (U) Reproduction of this document is authorized for official use only, in accordance with guidelines for reproduction of classified material outlined in Department of Defense (DOD) 5200.1-R, Information Security Program

RECORD OF CHANGES

Change Number	Copy Number	Date of Change	Date Posted	Posted By

**SECRET**

178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199

(INTENTIONALLY BLANK)

**SECRET**

viii



**SECRET**

HEADQUARTERS, U.S. STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE NE 68113-6500  
28 February 2008

200  
201  
202  
203  
204  
205  
206

USSTRATCOM CONPLAN 8039-08 (U)  
Classification Guidance (U)

<b>SUBJECT REQUIRING PROTECTION:</b>	<b>PROTECTION REQUIRED DURING:</b>			
	COA DEVELOP- MENT	EXEC- UTION PLANNING	IMPLEMEN- TATION	POST IMPLEMEN- TATION
(U) Plan Short Title	U	U	U	U
(U) Plan Long Title	U	U	U	U
(U) Cyberspace Terminology	S//REL	S//REL	S//REL	S//REL
(U) Threat Information	S//REL	S//REL	S//REL	S//REL
(U) Concept of Operations	S	S	S	S
(U) Classification Guide	S//REL	S//REL	U	U
(U) Communications effectiveness, sustainability, and limitations	S//REL	S//REL	U	U
(U) Command Arrangements and agreements	S//REL	S//REL	S//REL	S//REL
(U) Rules of Engagement (ROE)	S	S	S	S
(U) Assigned Areas of Operation and boundaries	S	S	S	S
(U) Key planning assumptions	S//REL	S//REL	S//REL	S//REL
(U) Operational constraints	S//REL	S//REL	S//REL	U

207  
208

**SECRET**

**SECRET**

209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230

(INTENTIONALLY BLANK)

**SECRET**

**SECRET**

HEADQUARTERS U.S. STRATEGIC COMMAND  
OFFUTT AFB NE 68113-6500  
28 February 2008

231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276

USSTRATCOM CONPLAN 8039-08 (U)  
Executive Summary (U)

1. (S) Situation.

a. (S) General. Commander, US Strategic Command  
(CDRUSSTRATCOM) CONPLAN 8039 CYBERSPACE OPERATIONS  
responds to Contingency Planning Guidance FY 05 and CJCSI

3110.01E (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) (CONPLAN 8039 also responds to draft  
Guidance for Employment of the Forces 08 (GEF) and draft Joint  
Strategic Capabilities Plan FY 08.) The plan provides a concept for

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) Further, CONPLAN 8039 provides cyberspace  
planners with a basis for (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) The plan's  
success hinges on close coordination among all Combatant  
Commanders, (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) operations. To facilitate and expedite planning, the  
plan consolidates existing roles, responsibilities, authorities, and  
rules of engagement from existing policy and guidance, which  
require CDRUSSTRATCOM coordinate with affected DOD  
components. In short the plan (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) Finally, a  
close working relationship with the interagency is critical  
throughout all phases of planning and execution, as the (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

b. (S) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322

The prosperity and security of our nation rely on (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) In short (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) security environment,  
CONPLAN 8039 supports the National Defense Strategy by  
providing (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

c. (S) Area of Concern. CDRUSSTRATCOM has no geographic area of responsibility (AOR) for normal operations (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)  
CDRUSSTRATCOM's area of interest (AOI) for military operations is global, particularly involving operations that transcend GCC boundaries. CDRUSSTRATCOM will work in full partnership with geographic combatant commanders (GCCs) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

CDRUSSTRATCOM must be prepared to support operations as directed by the President and Secretary of Defense (SECDEF) as well as to support other combatant commanders (CCDRs). Forces under CONPLAN 8039 (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

d. (S) Scope. CONPLAN 8039 is (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) When CONPLAN 8039 (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) For  
(b)(1) Sec 1.4(a) not currently covered in  
(b)(1) Sec 1.4(a) CONPLAN 8039 provides a framework for planning  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) This CONPLAN (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) effort among USSTRATCOM  
components. Since (b)(1) Sec 1.4(a) is collaboratively developed with

323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368

the GCCs, (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) ensures unity of purpose with all (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(1) (U) (b)(1) Sec 1.7(e)

(a) (S) The purpose of (b)(1) Sec 1.4(a) is to provide national leadership (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) Department of Defense (DOD) and US Government (USG) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(b) (S) Comprehensive and tailored (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) combatant commands and interagency partners.

(c) (S) (b)(1) Sec 1.4(a) encompass a (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) USG policy, and reflects combatant command collaboration. These appendices translate (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) They also translate (b)(1) Sec 1.4(a)

(d) (S) Depending on the level of planning, each (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) requirements, tasks, (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) and assessments of risk and effects.

e. (U) Friendly Forces.

(1) (U) Center of Gravity. For the purposes of CONPLAN 8039, COG analysis will cover CDRUSSTRATCOM's ability to conduct

369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414

operations in and through cyberspace. The US utilizes

(b)(1) Sec 1.7(e)

(2) (U) Strength and Composition. CDRUSSTRATCOM has Combatant Command (Command Authority) (COCOM) for forces delineated in Forces for Unified Commands (FY 2006) and Global Force management Guidance (FY 2005). CDRUSSTRATCOM will plan with all forces reasonably deemed essential to meet objectives.

f. (~~S//Rel to USA, AUS, GBR~~) Legal Considerations. CONPLAN 8039 contemplates military actions

(b)(1) Sec 1.4(a)

of US law, including the US Constitution, applicable US statutes, executive orders and regulations, the Law of Armed Conflict (LOAC), and applicable ROE.

(b)(1) Sec 1.4(a)

2. (~~S//Rel to USA, AUS, GBR~~) Mission.

a. (~~S//Rel to USA, AUS, GBR~~) Purpose. This concept plan provides a

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) In order to accomplish this, CONPLAN 8039 will perform the following four functions:

(1) (U) Provide context for a common planning structure by establishing linkages among cyberspace operations and operations in all environments.

(2) (~~S//Rel to USA, AUS, GBR~~) Provide methods to

(b)(1) Sec 1.4(a)

415 (3) (S//Rel to USA, AUS, GBR) Clarify (b)(1) Sec 1.4(a) roles and  
416 responsibilities from existing guidance to (b)(1) Sec 1.4(a)  
417 (b)(1) Sec 1.4(a)

418  
419 (4) (U) Describe operations and defense of the Global Information  
420 Grid

421  
422 b. (S//Rel to USA, AUS, GBR) Mission Statement Commander, US  
423 Strategic Command (b)(1) Sec 1.4(a)  
424 (b)(1) Sec 1.4(a)  
425  
426 support of national and military objectives, (b)(1) Sec 1.4(a)  
427 (b)(1) Sec 1.4(a)  
428

429 \*(U) Note: (b)(1) Sec 1.7(e)  
430 (b)(1) Sec 1.7(e)  
431  
432

433  
434 c. (U) (b)(1) Sec 1.7(e) CONPLAN 8039 is designed to  
435 support (b)(1) Sec 1.7(e) derived from  
436 (b)(1) Sec 1.7(e)  
437  
438 (b)(1) Sec 1.7(e) in CONPLAN  
439 8039. (b)(1) Sec 1.7(e)  
440 (b)(1) Sec 1.7(e)  
441  
442 (b)(1) Sec 1.7(e) CONPLAN 8039  
443 (b)(1) Sec 1.7(e)

444 (b)(1) Sec 1.7(e) CONPLAN 8039 also develops a  
445 structure for pre-planned authorities for (b)(1) Sec 1.7(e)  
446 (b)(1) Sec 1.7(e)  
447

448 (1) (S) (b)(1) Sec 1.4(a)  
449 (b)(1) Sec 1.4(a)

450  
451 (2) (S) (b)(1) Sec 1.4(a)  
452 (b)(1) Sec 1.4(a)

453  
454 (3) (S) (b)(1) Sec 1.4(a)  
455 (b)(1) Sec 1.4(a)

**SECRET**

456 3. (S) Execution.

457

458

a. (U) Commander's Intent. USSTRATCOM (b)(1) Sec 1.7(e)

459

(b)(1) Sec 1.7(e)

460

three scenarios:

461

462

(1) (U) When CDRUSSTRATCOM is the supported commander for planning within the context of other STRATCOM plans (e.g.

463

464

(b)(1) Sec 1.7(e) In this case,

465

(b)(1) Sec 1.7(e)

466

467

468

(2) (U) When CDRUSSTRATCOM is a supporting commander for another combatant commander, effects and supporting activities in support of other plans will be derived via the applicable combatant commander plan. For timing and tempo of operations, USSTRATCOM's assigned forces will follow the phasing or planned construct resident in that plan.

469

470

471

472

473

474

475

(3) (U) When CDRUSSTRATCOM is the supported commander,

476

CONPLAN 8039 (b)(1) Sec 1.7(e)

477

(b)(1) Sec 1.7(e)

478

479

b. (S) Concept of Operations. This CONPLAN employs the JP 5-0 (b)(1) Sec 1.4(a)

480

(b)(1) Sec 1.4(a) in and

481

through cyberspace. As necessary, and when required,

482

USSTRATCOM will modify the (b)(1) Sec 1.4(a)

483

reflect the concept of operations. The following paragraphs

484

describe general activities that relate to (b)(1) Sec 1.4(a) These

485

descriptions are general in nature and may or may not apply to all

486

(b)(1) Sec 1.4(a) CONPLAN 8039 describes the

487

(b)(1) Sec 1.4(a)

488

489

490

491

492

493

494

(S) It is essential that CONPLAN 8039 (b)(1) Sec 1.4(a) be utilized

495

in concert with Geographic Combatant Commander (GCC)

496

campaign plans. CONPLAN 8039 provides planning structure and

497

context, but is not intended to address (b)(1) Sec 1.4(a)

498

(b)(1) Sec 1.4(a)

499

(b)(1) Sec 1.4(a) CONPLAN 8039 is intended to serve as a tool for

500

developing executable OPLANs and EXORDs. For planning

501

purposes, the (b)(1) Sec 1.4(a) construct below allows for the systematic



502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547

arrangement of activities and tasks in a logical and anticipated sequence. Some activities from a given (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

(1) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) When CONPLAN 8039 (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(2) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) When CONPLAN 8039 (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) both cyber and non-cyber, are available for planners to quickly bundle into COAs to present to decision makers.

(3) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
Baseline (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) Planning and options for (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) are developed and fielded as directed.  
(b)(1) Sec 1.4(a)

(4) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) achieve specified objectives. (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(5) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577

(6) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

4. (U) Administration & Logistics.

a. (U) Concept of Support. Security, logistics, personnel and administrative support will be furnished by supporting commands in accordance with service directives, command arrangement agreements (CAAs), memoranda of understanding (MOU), Task Force (TF) operating instructions and the logistics concept for support operations outlined in CDRUSSTRATCOM plans and directives.

5. (U) Command & Control: Service cyberspace operations Command & Control (C2) structure, as it applies to USSTRATCOM and its components, (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)  
differently. See Annex J for C2 specifics regarding organizational structure expected (b)(1) Sec 1.7(e)  
for command relationships by scenario.

**SECRET**

HEADQUARTERS U.S. STRATEGIC COMMAND  
OFFUTT AFB NE 68113-6500  
28 February 2008

578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623

Terms of Reference

(U) CDR USSTRATCOM CONPLAN 8039-08

1. (U) Terms of Reference: Because of the relative newness of this warfare area, and due to a lack of consensus regarding terminology, failures in communication regarding cyberspace are common. The terms, phrases and figures below are intended to provide a usable, readily available and common vocabulary for the cyberspace planner. This listing is not intended to be all-inclusive or doctrinal, but rather to identify and reference doctrine where available, and to provide an explanation and common context for other terms used throughout this document.

- (U) Access: Sufficient level (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

- (U//FOUO) (b)(1) Sec 1.7(e) For the purposes of CONPLAN 8039, attacks  
(b)(1) Sec 1.7(e)

- o (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

- o (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669

- (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)
- o (b)(1) Sec 1.7(e)  
combination of such effects.
- o (b)(1) Sec 1.7(e)
- o (b)(1) Sec 1.7(e)
- o (b)(1) Sec 1.7(e)  
adversely affected.
- (U) Computer Network Defense Response Actions (CND-RAs, or RAs): RAs are deliberate, authorized measures or activities that protect and defend DOD computer systems and networks under attack or targeted for attack by adversary computer systems/networks. RAs extend DOD's layered defense-in-depth capabilities and increase DOD's ability to withstand adversary attacks. Objectives for using RAs include:
  - o (b)(1) Sec 1.7(e)
  - o (b)(1) Sec 1.7(e)
  - o (b)(1) Sec 1.7(e)
- (U) Computer Network Operations (CNO): Comprised of computer network attack (CNA), computer network defense (CND), and related computer network exploitation enabling operations (CNE). (JP 3-13). Note that for the purposes of CONPLAN 8039, Computer Network Operations and its subcategories are considered as (b)(1) Sec 1.7(e)

**SECRET**

670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715

(b)(1) Sec 1.7(e)

- (U) Computer Network Attack (CNA): Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 3-13)
- (U) Computer Network Defense (CND): Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks. (JP 6-0)
- (U) Computer Network Exploitation (CNE): Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. (JP 3-13)
- (U) Cross Domain Solution: An information assurance solution that provides the ability to manually and/or automatically access and/or transfer between two or more differing security domains. (CJCSI 6211.02b, DISN Policy, Responsibilities and Processes)
- (U) Cyber: Adjective form of cyberspace. Used as a modifier to create appropriate cyberspace related terms (cyber attack, cyber defense, cyber weapon, etc.)
- (U) (b)(1) Sec 1.7(e)
- (b)(1) Sec 1.7(e)
- (b)(1) Sec 1.7(e)
- (b)(1) Sec 1.7(e)
- (U) Cyber Attack Weapon Characterization: The process of determining and documenting the effect producing mechanisms and assurance factors of cyber attack weapons. Characterization

716 includes aspects of CNA technical assurance evaluation,  
717 Operational Test and Evaluation (OT&E), risk/protection  
718 assessments, and other screening processes. The operational risk  
719 assessment of employing or releasing an offensive or defensive  
720 cyber weapon shall include risk factors addressing safety (which  
721 can also be global and public) and security (loss of a weapon or  
722 exposure of a leading edge capability). Answers the question:  
723 "What do I need to know about this weapon before I can use it?"

724 (b)(1) Sec 1.7(e)

726  
727 - (S) (b)(1) Sec 1.4(a)

728 (b)(1) Sec 1.4(a)

732  
733 - (U) (b)(1) Sec 1.7(e) The extent to which the cyber

734 (b)(1) Sec 1.7(e)

736  
737 - (U) (b)(1) Sec 1.7(e) The manner in which a

738 (b)(1) Sec 1.7(e)

743  
744 - (U) (b)(1) Sec 1.7(e) A combination of one or more

745 (b)(1) Sec 1.7(e)

749  
750 - (U) (b)(1) Sec 1.7(e)

751 (b)(1) Sec 1.7(e)

- 754 ○ (b)(1) Sec 1.7(e)
- 755
- 756
- 757
- 758 ○
- 759
- 760
- 761

762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807

○ (b)(1) Sec 1.7(e)

- (U) (b)(1) Sec 1.7(e) The process of taking an  
(b)(1) Sec 1.7(e)

- (U) Cyber Capability: A capability (e.g., device, weapon, tool, computer program, or technique), including any combination of software, firmware, and hardware designed specifically to create an effect in or through cyberspace. Not all cyber capabilities are weapons or potential weapons.

- (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

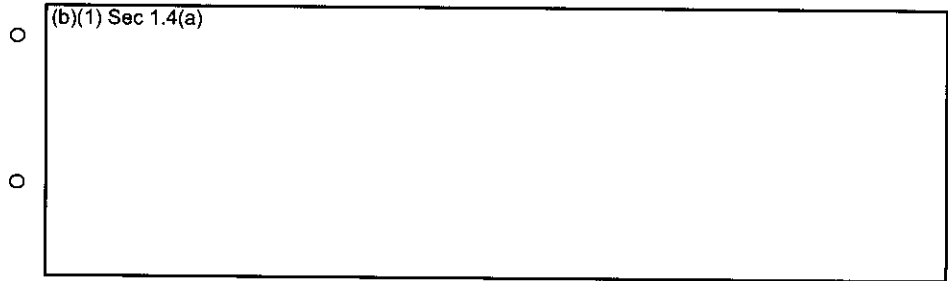
○ (b)(1) Sec 1.4(a)

○

○

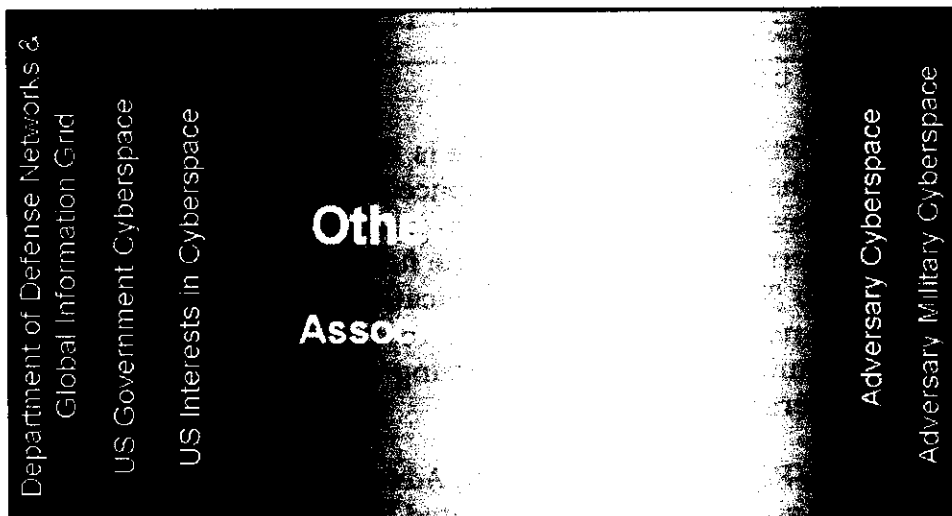
○

808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841



- (U) Cyberspace (working definition): A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. (working definition from NMS-CO)
  
- (U//~~FOUO~~) Cyberspace Defense: The goal of cyberspace defensive operations is to preserve the intended purpose and operating capabilities of a given network or system. Cyberspace defense is accomplished by a layered, defense-in-depth posture with mutually supporting elements of digital, electronic and physical protection. Critical infrastructure protection, Information Assurance and Computer Network Defense efforts all contribute to a robust defensive posture. Because of the extensive interconnections amongst networked systems, this variety of efforts supports protection of mission critical hardware and software, switching nodes, communications pathways and data integrity not only for critical Department of Defense networks, but also for portions of US, allied and civilian networks.
  
- (U) Cyberspace Domain: For the purposes of CONPLAN 8039, cyberspace is a domain using electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. (Per the NMS CO working definition of cyberspace)





(U) Figure 1: Cyberspace domain - Terrain

842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869

- (U) US Military Cyberspace: This is the area in Figure 1 delineated by the label "Department of Defense Networks & Global Information Grid". The GIG is as defined in Joint Publication (JP) 1-02. The GIG supports all DOD, national security, and related intelligence activities missions and functions (strategic, operational, and tactical), in war and in peace. DOD Networks span the full range from tactical battlefield data networks to networked strategic control systems.
- (U) US Cyberspace: This is the area in Figure 1 delineated by the label "US Government Cyberspace". Per the 2004 National Response Plan, all nationally owned cyberspace that resides outside of the DOD GIG is in this category and falls under the Department of Homeland Security (DHS) for protection. DHS responsibilities are detailed in the National Response Plan (NRP), 2004. This includes both U.S. owned and other U.S. government networks, across the full range of the interagency.
- (U) US Interests in Cyberspace: This is the area in Figure 1 delineated by the label "US Interests in Cyberspace". Networks and systems within this area are owned and operated by a variety of commercial, civil and other entities, however, the impact of their operation is of specific interest for the maintenance of national business operations. This category includes systems such as; (b)(1) Sec 1.7(e)

**SECRET**

870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915

(b)(1) Sec 1.7(e) financial, commerce and utility networks.

- (U) Other Cyberspace: This is the area in Figure 1 delineated by the label "Other Cyberspace and Associated Infrastructure". The vast majority of cyberspace lies within this region. Included are the full spectrum of World Wide Web (WWW) accessible applications and services, as well as the necessary global infrastructure to support communication and processing of the data flow that enables cyberspace.

- (~~S//Rel to USA, AUS, GBR~~) Adversary Cyberspace: This is the area in Figure 1 delineated by the label "Adversary Cyberspace". Included are those portions of cyberspace

(b)(1) Sec 1.4(a)

- (U) Adversary Military Cyberspace: This is the area in Figure 1 delineated by the label "Adversary Military Cyberspace".

(b)(1) Sec 1.7(e)

- (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

8039 characterizes (b)(1) Sec 1.4(a)

- (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Comprised of:

- (b)(1) Sec 1.4(a)
- 

- (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) May require (b)(1) Sec 1.4(a) Comprised of:

- (b)(1) Sec 1.4(a)
- 

- (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) May require (b)(1) Sec 1.4(a) Comprised of:

916  
917  
918  
919  
920

- (b)(1) Sec 1.4(a)
- 
- 

Unclassified

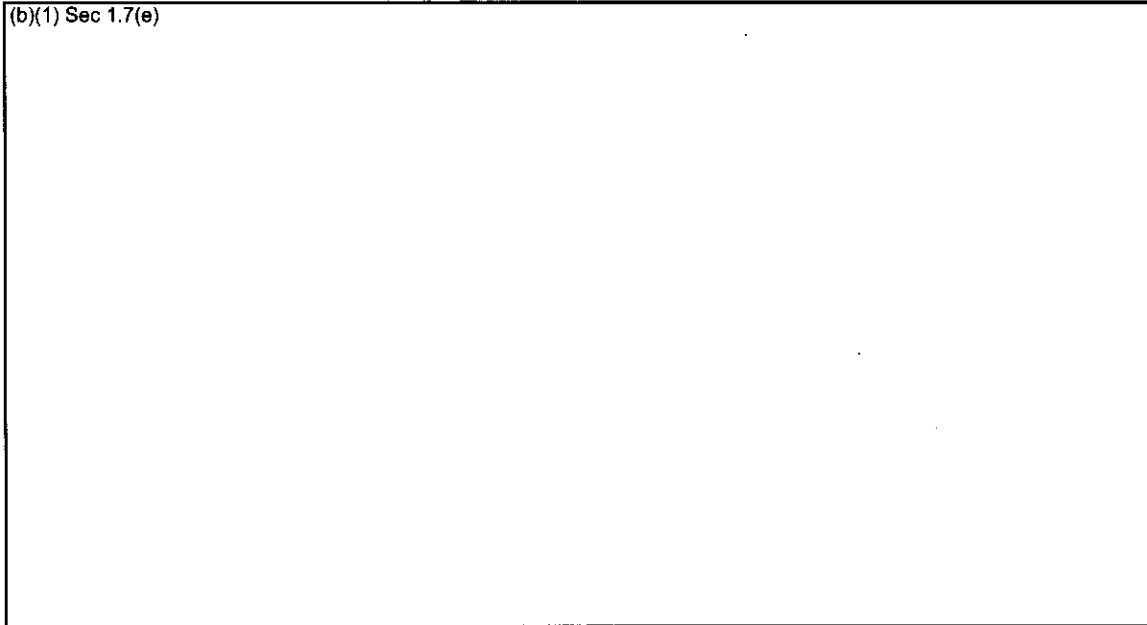


Figure 2: (U) Cyberspace (b)(1) Sec 1.7(e)

921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933

- (U) Cyberspace elements: For the purpose of CONPLAN 8039, there are four elements that comprise military use of cyberspace – Purpose, Infrastructure, Electromagnetic Spectrum, and Data. Arranging the elements of cyberspace into a cyber triangle (see Figure 3, below) helps to clarify the four separate, but related, aspects of cyberspace systems. After determining the desired objectives, effects, and actions, planners can use the triangle as a (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) Analysis of the cyber triangle can also guide the search for critical vulnerabilities.

UNCLASSIFIED

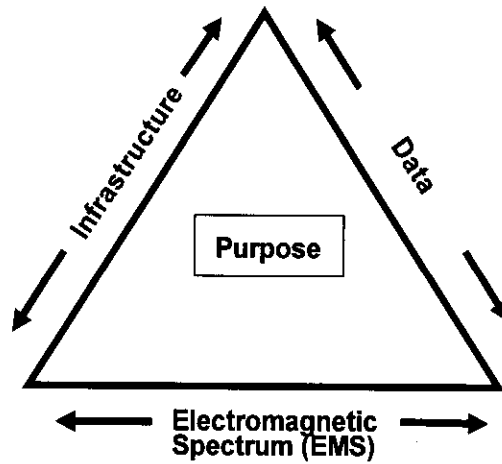


Figure 3: (U) Cyberspace Elements  
The Cyber Triangle

934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959

- (U) Purpose. This central element represents the reason that an actor uses cyberspace to further his objectives. If an adversary doesn't see the value in using cyberspace to further his objectives hostile to the United States, his cyberspace capability (the rest of the cyber triangle) is not relevant. (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

- (U) Infrastructure. For the purposes of this plan, infrastructure includes the "global information infrastructure" as defined in JP 1-02 (see below) as well as

(b)(1) Sec 1.7(e)

- (U) Electromagnetic Spectrum (EMS). EMS refers to the range of frequencies of electromagnetic radiation from zero to infinity. It can be measured in cycles per second or wavelength in centimeters and includes radio waves, microwaves, and all forms of radiated energy.

**SECRET**

- 960           ○ (U) Data: Representation of facts, concepts or instructions in  
961           a formalized manner suitable for communication,  
962           interpretation or processing by humans or automatic means.  
963           (JP 1-02) For the purposes of this plan, data refers to any  
964           such information that can be created, stored, modified, or  
965           exchanged via networked systems and associated  
966           infrastructure, as given in the NMS-CO.  
967
- 968       - (U) Cyberspace Operations: Actions taken in, and extending  
969       through cyberspace, transcending Computer Network Operations  
970       (CNO). Cyberspace Operations broadly include the following  
971       objectives:  
972
- 973           ○ (S) (b)(1) Sec 1.4(a) [redacted]  
974           (b)(1) Sec 1.4(a) [redacted]
- 975
- 976           ○ (S) (b)(1) Sec 1.4(a) [redacted]
- 977
- 978           ○ (S) (b)(1) Sec 1.4(a) [redacted]  
979           (b)(1) Sec 1.4(a) [redacted]
- 980
- 981       - (U) Cyberspace Superiority: The degree of dominance in  
982       cyberspace of one force over another that permits the conduct of  
983       operations by the former, and its related air, land, sea and space  
984       forces at a given time and place without prohibitive interference by  
985       the opposing force. (Adapted from: JP 3-13, 3-14, 3-30,  
986       Information, Space and Air Superiority)  
987
- 988       - (U) Cyber Warfare: Direct creation of effects in and through  
989       cyberspace in support of a combatant commander's military  
990       objectives. Comprises operations conducted to guarantee friendly  
991       forces freedom of action in cyberspace while denying opposing  
992       forces effective use of cyberspace.  
993
- 994       - (U) Data: Representation of facts, concepts, or instructions in a  
995       formalized manner suitable for communication, interpretation, or  
996       processing by humans or by automatic means. Any  
997       representations such as characters or analog quantities to which  
998       meaning is or might be assigned. (JP 1-02)  
999
- 1000           ○ For the purposes of CONPLAN 8039, data refers to any  
1001           information, consistent with the above definition, which can  
1002           be created, stored, modified, or exchanged via networked  
1003           systems and associated infrastructure.  
1004

**SECRET**

- 1005 – (U) Deny: To degrade, disrupt, or destroy access to, operation of,  
1006 or availability of a target by a specified level for a specified time.  
1007 Denial is concerned with preventing adversary use of resources.  
1008
- 1009 – (U) Degrade: (a function of amount) To deny access to or  
1010 operation of a target to a level represented as a percentage of  
1011 capacity. Level of degradation must be specified. If a specific time  
1012 is required, it can be specified, otherwise start and stop-time are  
1013 assumed to be indeterminate.  
1014
- 1015 – (U) Destroy: To permanently, completely, and irreparably deny  
1016 access to, or operation of, a target. Destruction is the denial effect  
1017 where time and amount are both maximized.  
1018
- 1019 – (U) Digital Protection: Actions taken in cyberspace to protect,  
1020 defend, monitor, analyze, detect and respond to unauthorized  
1021 network activity. It encompasses the concepts of Computer  
1022 Network Defense (CND), Information Assurance (IA), and Response  
1023 Actions (RAs).  
1024
- 1025 – (U) Disrupt: (a function of time) To completely but temporarily  
1026 deny access to or operation of a target for a period represented as a  
1027 function of time. A desired start and stop time are normally  
1028 specified. Disruption can be considered a special case of  
1029 degradation where the degradation level selected is 100%.  
1030
- 1031 – (U) Effects Assessment: The timely and accurate evaluation of  
1032 effects resulting from the application of lethal or nonlethal force  
1033 against a military objective. Effect assessment can be applied to  
1034 the employment of all types of weapon systems (air, ground, naval,  
1035 special forces, and cyber weapon systems) throughout the range of  
1036 military operations. (b)(1) Sec 1.7(e)  
1037 responsibility with required inputs and coordination from the  
1038 operators. Effects assessment is composed of physical effect  
1039 assessment, functional effect assessment, and target system  
1040 assessment. Note: Battle Damage Assessment (BDA) is a specific  
1041 type of effects assessment for damage effects. (Adapted from the  
1042 JP 1-02 definition of BDA.)  
1043
- 1044 – (U) Electronic Protection: Division of electronic warfare involving  
1045 actions taken to protect personnel, facilities, and equipment from  
1046 any effect of friendly or enemy use of the electromagnetic spectrum  
1047 that degrades, neutralizes, or destroys friendly combat capability.  
1048 (JP 3-13.1)  
1049

**SECRET**

XXX

**SECRET**

- 1050 – (U) Friendly Cyberspace: Those portions of cyberspace used,  
1051 controlled, and/or maintained by entities understood to be non-  
1052 hostile to the US, its allies, or coalition partners. For instance, the  
1053 GIG, our military data links, and critical US cyber infrastructure  
1054 are examples of friendly cyberspace.  
1055
- 1056 – (U) Global Information Grid (GIG): The globally interconnected,  
1057 end-to-end set of information capabilities, associated processes  
1058 and personnel for collecting, processing, storing, disseminating,  
1059 and managing information on demand to warfighters, policy  
1060 makers, and support personnel. The Global Information Grid  
1061 includes owned and leased communications and computing  
1062 systems and services, software (including applications), data,  
1063 security services, other associated services and National Security  
1064 Systems. Also called GIG. (JP 6-0)  
1065
- 1066 – (U) Global Information Infrastructure (GII): The worldwide  
1067 interconnection of communications networks, computers,  
1068 databases, and consumer electronics that make vast amounts of  
1069 information available to users. The global information  
1070 infrastructure encompasses a wide range of equipment, including  
1071 cameras, scanners, keyboards, facsimile machines, computers,  
1072 switches, compact disks, video and audio tape, cable, wire,  
1073 satellites, fiber-optic transmission lines, networks of all types,  
1074 televisions, monitors, printers, and much more. The friendly and  
1075 adversary personnel who make decisions and handle the  
1076 transmitted information constitute a critical component of the  
1077 global information infrastructure. Also called GII. (JP 3-13)  
1078
- 1079 – (U) HVAC: Heating, Ventilation and Air Conditioning. An acronym  
1080 used to describe equipment used to control the temperature and  
1081 humidity of an enclosed space. HVAC systems are critical for the  
1082 efficient operation of computer and network equipment to maintain  
1083 their operating environment within required specifications.  
1084
- 1085 – (U) Infrastructure: For the purposes of CONPLAN 8039,  
1086 infrastructure is the superset of systems including the GII (see  
1087 above) (b)(1) Sec 1.7(e)  
1088 (b)(1) Sec 1.7(e)  
1089  
1090  
1091  
1092
- 1093 – (U) Intended Cyber Effect: A sorting of cyber capabilities into  
1094 broad operational categories based on the outcomes they were  
1095 designed to create. These categories are used to guide capability

**SECRET**

1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140

selection decisions. Answers the question: "What kind of capability is this?" Specifically:

- Denial: degrade, disrupt, or destroy access to, operation, quality of service, or availability of target resources, processes, and/or data.
- (b)(1) Sec 1.7(e)
- Command and Control: provide operator control of deployed cyber capabilities.
- Information/Data Collection: obtain targeting information about targets or target environments.
- Access: establish unauthorized access to a target.
- Enabling: provide resources or create conditions that support the use of other capabilities.

- (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

- (U) Lethal: Causing death or permanent injuries to personnel.

- (U) Malware: Software designed to infiltrate or damage a computer system without the owner's informed consent. It is a combination of the words "malicious" and "software". The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

- (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

- (U) Misfire: The failure of a weapon to take its designed action; failure of a primer, propelling charge, transmitter, emitter, computer software, or other munitions component to properly function, wholly or in part. (Note: adapted from the JP 1-02 definition of misfire.)



**SECRET**

- 1141 - (U) Nonkinetic: Refers to actions which do not use forces of  
1142 dynamic motion and/or energy upon material bodies. See (b)(1) Sec 1.7(e)  
1143 (b)(1) Sec 1.7(e)  
1144
- 1145 - (U) Nonlethal: Neutralizing or incapacitating a target without  
1146 causing death or permanent injury to personnel. Nonlethal refers  
1147 to being relatively reversible and is not required to have zero  
1148 probability of causing fatalities or permanent injuries.  
1149
- 1150 - (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
1151 (b)(1) Sec 1.4(a)  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173
- 1174 - (U) Physical protection: Preservation of the effectiveness and  
1175 survivability of mission-related military and nonmilitary  
1176 equipment, facilities, and infrastructure deployed or located within  
1177 or outside the boundaries of a given area. (Adapted from JP 3-0)  
1178
- 1179 - (U) Probability of Effect (PE): The chance of a specific functional or  
1180 behavioral impact on a target given a weapon action.  
1181
- 1182 - (U) Response Actions (RA): See "Computer Network Defense  
1183 Response Actions" above.  
1184
- 1185 - (U) (b)(1) Sec 1.7(e)  
1186 acronym used to describe (b)(1) Sec 1.7(e) which are used to

**SECRET**

1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227

(b)(1) Sec 1.7(e)

accessible internet.

- (U) Target State: The condition of a target described with respect to a military objective or set of objectives.
- (U) Targeted Vulnerability: An exploitable weakness in the target required by a specific weapon.
  - o Objective Vulnerability: A vulnerability whose exploitation directly accomplishes part or all of an actual military objective.
  - o Access Vulnerability: A vulnerability whose exploitation allows access to an objective vulnerability.
- (U) Weapon Action: The effect-producing mechanisms or functions initiated by a weapon when triggered. (e.g., the weapon actions of a kinetic weapon are blast, heat, fragmentation; (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

- (U) Weapon Effect: A direct or indirect (intended or unintended) outcome of a weapon action. In warfare, the actions of a weapon are employed to create intended effects, typically to the functional capabilities of a material or personnel target or to the behavior of individuals.
  - o Direct Effect: An outcome that is immediately caused by the weapon's action. Also known as a first order effect.
  - o Indirect Effect: An outcome that cascades from one or more direct effects; the outcome may be several degrees away from the direct effect but the direct effect must be the proximate cause of the eventual outcome. Also known as second order effects, third order effects, etc.

**SECRET**

1228 HEADQUARTERS, U.S. STRATEGIC COMMAND  
1229 OFFUTT AIR FORCE BASE NE 68113-6500  
1230 28 February 2008  
1231

1232 USSTRATCOM CONPLAN 8039-08 (U)

1233 Base Plan (U)

1234

1235 1. References:

1236

1237 a. (U) CJCSM 3122.03C, Joint Operation Planning and Execution  
1238 System (JOPES) Volume II, Planning Formats and Guidance,  
1239 (Current as of 17 August 2007)

1240

1241 b. (U) CJCSM 3122.01, Joint Operation Planning and Execution  
1242 System (JOPES) Volume I (Planning Policies and Procedures), 29  
1243 Sep 06 (Current as of 6 December 2007)

1244

1245 c. (U) CJCSI 3110.01F, Joint Strategic Capabilities Plan (TS), 1 Sep  
1246 06

1247

1248 d. (U) Joint Pub 1, Doctrine for the Armed Forces of the United  
1249 States, 14 May 2007

1250

1251 e. (U) SM-712-89 Unified Command Plan (UCP) (S), 5 May 06

1252

1253 f. (U) Defense Planning Guidance (DPG), FY 2004-2009 (S), May 02

1254

1255 g. (U) CDRUSSTRATCOM Implementation Plan (IPLAN) for assuming  
1256 the Computer Network Defense (CND) Mission, 14 May 99

1257

1258 h. (U) Draft Strategic Guidance Statement for Computer Network  
1259 Operations (S), 24 Apr 06

1260

1261 i. (U) Computer Network Attack Implementation Plan (S//NF), 26  
1262 Jan 00

1263

1264 j. (U) Computer Network Attack Concept of Operations (S//NF), 30  
1265 Jun 00

1266

1267 k. (U) Delegation of Disclosure Authority Letter, National Disclosure  
1268 Policy Committee Case No. 6005-00 – Multiple Countries (S), 7  
1269 Jun 00

1270

1271 1. (U) National Intelligence Estimate NIE 2004-01HC/I, Cyber  
1272 Threats to the United States Information Infrastructure (S//NF),  
1273 15 Mar 04

**SECRET**

**SECRET**

- 1274  
1275 m. (U) DODD 0-8530.1, Computer Network Defense (CND), 8 Jan 01  
1276  
1277 n. (U) CJCSM 3113.01A Series, "Theater Engagement Planning," 31  
1278 May 00 (current as of 25 May 05)  
1279  
1280 o. (U) CJCSI 3121.01B, Standing Rules of Engagement/Standing  
1281 Rules for the Use of Force for US Forces (S), 13 Jun 05 (Current as  
1282 of 5 July 2007)  
1283  
1284 p. (U) APPENDIX 12 TO ANNEX C (OPERATIONS) TO JTF GNO  
1285 OPOD 05-01 (Global Network Operations) INFORMATION  
1286 OPERATIONS CONDITION (INFOCON) EXECUTION  
1287 PROCEDURES (C//Rel USA, AUS, CAN, NZL), 22 May 06  
1288  
1289 q. (U) DODD O-8530.02, Support to Computer Network Defense, 9  
1290 Mar 01  
1291  
1292 r. (U) CJCS Homeland Security (HLS) Standing Execution Order  
1293 (S//Rel USA, CAN) 161950Z OCT 01  
1294  
1295 s. (U) CJCS Strategic Plan, National Military Strategy Plan for the  
1296 War on Terrorism, Revision 3 (TS), 032000Z Jan 2002  
1297  
1298 t. (U) Computer Network Defense (CND) Response Actions (RA)  
1299 Concept of Operations (S), Draft as of 6 May 04  
1300  
1301 u. (U) Guidance for Computer Network Defense (CND) Response  
1302 Actions (RA) Memorandum. Signed by (b)(6)  
1303 (U//FOUO), 26 Feb 03  
1304  
1305 v. (U) Contingency Planning Guidance (CPG) 2005 (TS)  
1306  
1307 w. (U) National Security Systems as defined in section 5142 of the  
1308 Clinger-Cohen Act of 1996  
1309  
1310 x. (U) National Military Strategy for Cyberspace Operations (S), 11  
1311 Dec 06  
1312  
1313 y. (U) Quadrennial Defense Review (S), 6 Feb 2006  
1314  
1315 z. (U) SECDEF Memorandum, Assignment and Delegation of  
1316 Authority to Director, Defense Information Systems Agency (DISA)  
1317 (U//FOUO), 18 Jun 04  
1318

**SECRET**

**SECRET**

- 1319 aa. (U) ASD 3CI Memorandum, DOD Guidance for Computer Network  
1320 Defense Response Actions (U//FOUO), 26 Feb 03  
1321 bb. (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
1322 (b)(1) Sec 1.4(a)  
1323  
1324  
1325 cc. (U) Horizontal Command and Control (C2) Integration (HC2I)  
1326 Concept of Operations (CONOPS) (S//Rel USA, AUS, CAN, NZL),  
1327 20 Dec 05  
1328  
1329 dd. (U) JTF-GNO OPORD 03-02 Reconnaissance and Surveillance  
1330 and Computer Network Defense (U//FOUO), 25 Mar 04  
1331  
1332 ee. (U) CJCSM 6510.01, Defense in Depth: Information Assurance  
1333 (IA) and Computer Network Defense (CND) (U//FOUO), 25 Mar 03.  
1334 Including Ch 2, 26 Jan 06, Ch 3, 8 Mar 06, (Current as of 14 Aug  
1335 2006)  
1336  
1337 ff. (U) JTF-GNO OPORD 05-01, Global Network Operations  
1338 (U//FOUO)  
1339  
1340 gg. (U) USSTRATCOM Planning Order (PLANORD) for Ongoing  
1341 Computer Network Intrusion Activities (S//Rel USA, AUS, GBR),  
1342 17 Oct 2005  
1343  
1344 hh. (U) Amplification to JFCC NW PLANORD (S//Rel USA, AUS,  
1345 GBR), 09 Mar 06  
1346  
1347 ii. (U) USSTRATCOM Joint Concept of Operations for Global  
1348 Information Grid NETOPS, 4 Aug 06  
1349  
1350 jj. (U) Forces for Unified Commands Memorandum, FY06 (S), 13 Jan  
1351 06  
1352  
1353 kk. (U) Trilateral Memorandum of Agreement among the Department  
1354 of Defense, the Justice Department and the Intelligence  
1355 Community Regarding Computer Network Attack and Computer  
1356 Network Exploitation Activities (DOD-JD-IC MOA) (S//NFS//NF),  
1357 9 May 07  
1358  
1359 ll. (U) Joint Task Force – Global Network Operations Implementing  
1360 Directive, 5 Aug 05  
1361  
1362 mm. (U) Joint Functional Component Command – Network  
1363 Warfare Implementing Directive, 20 Jan 05  
1364

**SECRET**

**SECRET**

- 1365 nn. (U) USSTRATCOM Network Warfare CONOP (S/Rel USA, AUS,  
1366 GBR), May 2006  
1367  
1368 oo. (U) (b)(1) Sec 1.7(e)  
1369 (b)(1) Sec 1.7(e) (S), 7 Jul 04  
1370  
1371 pp. (U) 2003 National Strategy for Securing Cyberspace (NS-SC)  
1372  
1373 qq. (U) 2003 National Strategy for the Physical Protection of Critical  
1374 Infrastructure and Key Assets, Feb 03  
1375  
1376 rr. (U) 2004 National Response Plan (NRP) Dec 04  
1377  
1378 ss. (U) Joint Publication 3-13, Information Operations, 13 Feb 06  
1379  
1380 tt. (U) Joint Publication 1-02, Department of Defense Dictionary of  
1381 Military and Associated Terms, 12 April 2001 (As Amended  
1382 Through 20 March 2006)  
1383  
1384 uu. (U) The Law of Armed Conflict, composed of International  
1385 Agreements to which the United States is a party and Customary  
1386 International Law binding on the United States  
1387  
1388 vv. (U) United States Code, Title 10, Armed Forces  
1389  
1390 ww. (U) United States Code, Title 18, Crimes and Criminal  
1391 Procedure  
1392  
1393 xx. (U) United States Code, Title 50, War and National Defense  
1394  
1395 yy. (U) United States Code, Title 32, National Defense  
1396  
1397 zz. (U) SECDEF Delegation of Authority to Appoint the Person  
1398 Serving as Director, National Security Agency, (DIRNSA) as  
1399 Commander, Joint Functional Component Command for Network  
1400 Warfare (JFCC NW) (S), 20 Jan 05  
1401  
1402 aaa. (U) Designation of the Director, Defense Information  
1403 Systems Agency (DISA), as Commander, Joint Task Force-Global  
1404 Network Operations (JTF-GNO), 17 Nov 05  
1405  
1406 bbb. (U) JFCC for Space Implementation Directive (U//FOUO),  
1407 19 Jul 06  
1408  
1409 ccc. (U) JFCC for Global Strike Integration (GSI) Implementation  
1410 Directive (U//FOUO), 19 Jul 06

**SECRET**

**SECRET**

- 1411
- 1412 ddd. (U) JFCC IMD Implementation Directive (U//FOUO), 22 Jan
- 1413 05
- 1414
- 1415 eee. (U) JFCC ISR Implementation Directive (U//FOUO), 24 Jan
- 1416 05
- 1417
- 1418 fff. (U) Strategic Command Directive 527-1, DOD Information
- 1419 Operations Condition (INFOCON) System Procedures (U//FOUO),
- 1420 27 Jan 06
- 1421
- 1422 ggg. (U) (U) CJCSM 3122.07A, IJSTO Supplement to Joint
- 1423 Operation Planning and Execution System (JOPES) (S//Rel USA,
- 1424 AUS, CAN GBR), 20 Oct 06
- 1425
- 1426 hhh. (U) Information Operations Roadmap (S//NF), 30 Oct 03
- 1427
- 1428 iii. (U) Doctrine for Joint Operation Planning, JP 5-0, 26 Dec 06
- 1429
- 1430 jij. (U) (U) (b)(1) Sec 1.7(e) for CONPLAN 8039 ),
- 1431 updated semiannually (S//SI//NF)
- 1432
- 1433 kkk. (U) Joint Publication 3-0, Joint Operations, 17 Sep 06
- 1434
- 1435 lll. (U) (b)(1) Sec 1.7(e)
- 1436 (b)(1) Sec 1.7(e) Sep 06
- 1437
- 1438 mmm. (U) 61JTCG/ME-1-8, Rev 1, Draft 2007, Requirements for
- 1439 Generating, Documentation, Reviewing, and Approving JTCG/ME
- 1440 Vulnerability Data.
- 1441
- 1442 nnn. (U) Deterrence Operations Joint Operating Concept, v 1.9,
- 1443 Jul 06
- 1444
- 1445 ooo. (U) Joint Publication 6-0, Joint Communications System, 20
- 1446 Mar 06
- 1447
- 1448 ppp. (U) CJCSI 5810.01C Implementation of the DOD Law of War
- 1449 Program, 31 Jan 07
- 1450
- 1451 qqq. (u) USSTRATCOM Operational Concept for Cyberspace (OCC)
- 1452 (DRAFT 2008)
- 1453
- 1454 rrr. (S) (b)(1) Sec 1.4(a)
- 1455 (b)(1) Sec 1.4(a)
- 1456

**SECRET**

1457 1. (U) Situation

1458

1459 a. (U) General

1460

1461 (1) (U) This is the United States Strategic Command  
1462 (USSTRATCOM) Concept Plan (CONPLAN) 8039 for Cyberspace  
1463 Operations (CO). The strategic goal of CONPLAN 8039 is to  
1464 ensure US military freedom of action in cyberspace and to be  
1465 able to deny adversary freedom of action in cyberspace. To  
1466 achieve this goal, (b)(1) Sec 1.7(e)

1467 (b)(1) Sec 1.7(e)  
1468  
1469  
1470  
1471  
1472

1473 cyberspace, when directed. Additionally, the plan calls on

1474 (b)(1) Sec 1.7(e)  
1475

1476 (b)(1) Sec 1.7(e) This plan is  
1477 prepared and submitted in accordance with requirements  
1478 detailed in references a and b, and supports the national  
1479 interests outlined in references c through bq.

1480

1481 (2) (U) (b)(1) Sec 1.7(e)

1482 (b)(1) Sec 1.7(e)  
1483

1484 (b)(1) Sec 1.7(e) The prosperity and security of our nation rely  
1485 on cyberspace to achieve and maintain strategic advantage and  
1486 strengthen the instruments of national power.

1487

1488 (3) (U) The scope of CONPLAN 8039 spans from peacetime through  
1489 war fighting in and through cyberspace. It does not direct but  
1490 must be able to (b)(1) Sec 1.7(e)

1491 (b)(1) Sec 1.7(e)  
1492  
1493  
1494

1495 b. (U) Areas of Concern. For the purposes of CONPLAN 8039,  
1496 cyberspace is a domain using electronics and the electromagnetic  
1497 spectrum to store, modify, and exchange data via networked  
1498 systems and associated physical infrastructures, per reference x.  
1499 Treating cyberspace as a domain (see Terms of Reference) provides  
1500 the "cyber-terrain" where 8039 operations will take place. Areas of  
1501 concern per reference c are:



**SECRET**

1502 (1) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
1503 this plan is considered to be (b)(1) Sec 1.4(a)  
1504 (b)(1) Sec 1.4(a) as described in the Terms of Reference (see Figure 1,  
1505 Terms of Reference) (b)(1) Sec 1.4(a)  
1506 (b)(1) Sec 1.4(a) by operations in  
1507 cyberspace (see the Terms of Reference for more detailed  
1508 discussion on the elements of cyberspace).

1509  
1510 (2) (U) Operational Area (OA). The potential operational area for  
1511 this plan is the entire cyberspace domain. The transregional,  
1512 global nature of cyberspace (b)(1) Sec 1.7(e)  
1513 operational area can (b)(1) Sec 1.7(e) and  
1514 wherever the Commander is directed to advance and defend US  
1515 interests in and through cyberspace. The operational area of  
1516 the plan consists of both the:

- 1517 ○ (b)(1) Sec 1.7(e) and
- 1518
- 1519 ○ (b)(1) Sec 1.7(e) as established by EXORD. For more  
1520 information on cyber engagement criterion, see Concept of  
1521 Operations below.

1522 Mission execution for CONPLAN 8039 is (b)(1) Sec 1.7(e)  
1523 objective driven, effects-based, and may be impacted from any  
1524 of the (b)(1) Sec 1.7(e)

1525 (b)(1) Sec 1.7(e)

1526  
1527  
1528 (see Figure 1, Terms of Reference). For detailed discussion on  
1529 each sub-area, see the 8039 Terms of Reference.

1530  
1531 c. (U) Effects in cyberspace. Effects in cyberspace can be generated  
1532 by influencing some or all of its elements, the constructs that  
1533 support these elements, or its intended purpose. See the Terms of  
1534 Reference for detailed discussion on the elements of cyberspace  
1535 (cyberspace triangle).

1536  
1537 d. (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Commander,  
1538 USSTRATCOM will utilize (b)(1) Sec 1.4(a)  
1539 (b)(1) Sec 1.4(a)  
1540 (b)(1) Sec 1.4(a) Example (b)(1) Sec 1.4(a)  
1541 (b)(1) Sec 1.4(a) are in Annex A, Appendix 3. (b)(1) Sec 1.4(a) (as defined in  
1542 the Terms of Reference) are presented in Annex C.

1543  
1544 e. (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) DOD must retain  
1545 (b)(1) Sec 1.4(a)

1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568

(b)(1) Sec 1.4(a)

(1) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(a) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) See Figure 4 (below).

1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

Figure 4: (S//REL to USA, AUS, GBR)

(b)(1) Sec 1.4(a)

1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580

(b) (U) Operational. See (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

(2) (U) Critical Factors.

(a) (U) Strategic.

1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

**SECRET**

1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595

(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) These  
capabilities can be (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) (as described in the Terms of  
Reference).

2 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) Ultimately, the goal of cyber  
warfare is to (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

Figure 3, Terms of Reference and Figure 5 below).

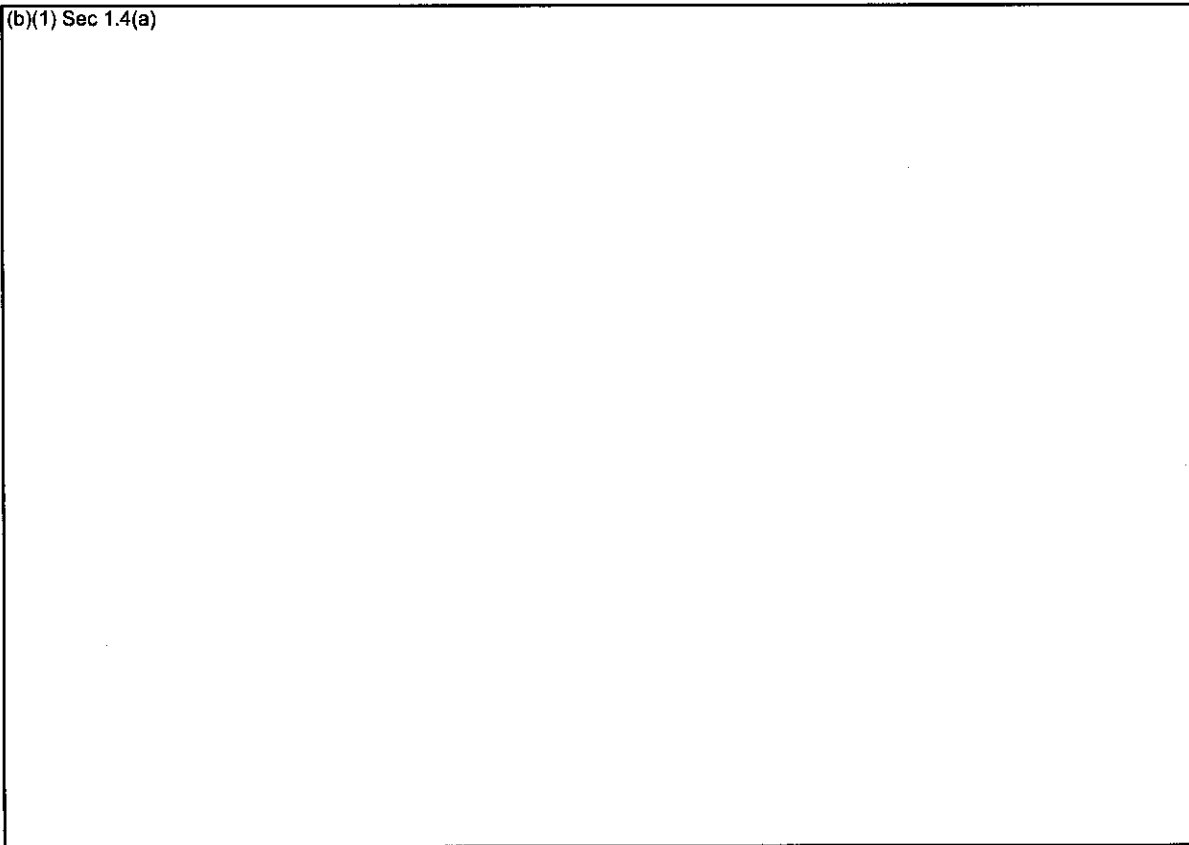


Figure 5:  
(~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

1596  
1597  
1598  
1599  
1600  
1601

a (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
In order to affect any element of cyberspace, the  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) More detailed discussions on

**SECRET**

**SECRET**

1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647

(b)(1) Sec 1.4(a) are found in Annex C. More detailed discussions covering (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) can be found in Annexes B & C.

b (U) Defensive considerations. Optimally, actors attempt to gain and maintain confidence in their use

(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) listed above). Operational planners

(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) Generally as systems become larger and more complex there are more opportunities to exploit.

c (U) The following rules apply to this methodology:

(1) (U) Primacy of purpose. The focus of attack on any cyberspace system is to affect that system's intended purpose. (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(2) (U) Cascading effects. Multiple attacks on varying elements can have cumulative effects and even a single attack can have cascading effects in, through and outside of the cyberspace domain.

d (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b) (U) Operational. See (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(3) (U) Courses of Action.

(a) (S//Rel to USA, AUS, GBR) General. Cyberspace threats are not limited to (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693

(b)(1) Sec 1.4(a)

(b) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The general

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) with respect to their effort. The

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) However, those potential adversaries who

(b)(1) Sec 1.4(a)

(c) (~~S//Rel to USA, AUS, GBR~~) Strategic Objectives. The principal strategic objectives of an adversary's offensive cyber operations are (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) This activity may fall into more than one category. See Annex B for a detailed discussion of adversary capabilities and general courses of action.

(d) (U) Operational Objectives. See (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) operational-level objectives.

f. (U) Friendly Forces.

(1) (U) Center of Gravity (COG).

(a) (~~S//Rel to USA, AUS, GBR~~) Strategic. For the purposes of CONPLAN 8039, COG analysis will cover

CDRUSSTRATCOM's (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) COGs and critical capabilities based on analysis conducted per ref bk.

1 (U) Leadership. Represents those individuals within DOD who can influence critical missions and processes within cyberspace. Senior Leadership includes the President of the United States (POTUS), the SECDEF and those subordinate officers appointed by POTUS and SECDEF.

**SECRET**

1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703

- 2 (U) Population. In this context is the aggregate of the US residents and their will to pursue national objectives and support leadership.
- 3 (U) Fielded Forces. Are those DOD forces/organizations who conduct military operations within cyberspace. Figure 6 (below) illustrates relationships between critical capabilities as crucial enablers for COGs.

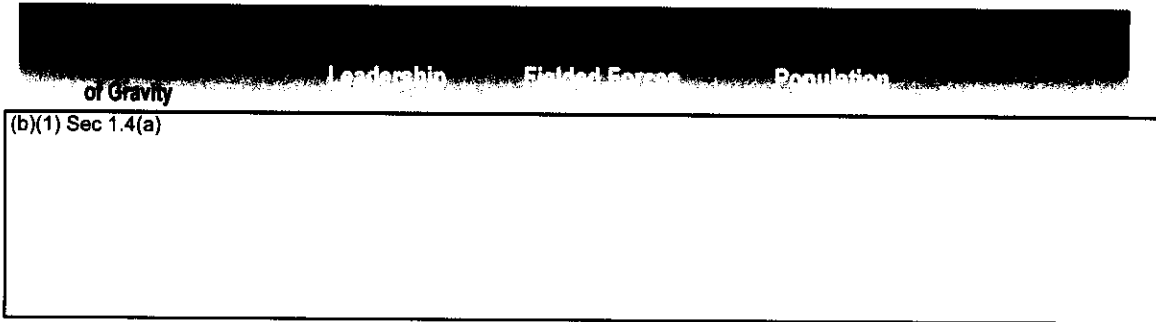


Figure 6: (~~S//REL to USA, AUS, GBR~~)  
Friendly Center of Gravity

1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727

- (b) (U) Operational. See Annex C for friendly operational-level COG analysis.
- (2) (U) Critical Factors.
  - (a) (U) Strategic.
    - 1 (~~S//Rel to USA, AUS, GBR~~) Friendly Critical Capabilities (CCs). The US utilizes cyberspace to enable the following functional critical capabilities (ref bk): (b)(1) Sec 1.4(a)
    - (b)(1) Sec 1.4(a)
    - (b)(1) Sec 1.4(a) (see Terms of Reference for cyberspace elements).
    - 2 (~~S//Rel to USA, AUS, GBR~~) Friendly Critical Vulnerabilities (CVs). Friendly CVs are (b)(1) Sec 1.4(a)
    - (b)(1) Sec 1.4(a)
- (b) (U) Operational. More detailed blue force operational critical factor analysis will be conducted in Annex C.

1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773

(3) (U) Composition. Friendly forces consist of combatant commands (CCDRs), allies, services and agencies. Outside of DOD, the Computer Emergency Response Teams (CERTs) and the DHS, law enforcement agencies (LEAs), and counterintelligence (CI) organizations collectively provide, manage, and maintain cyberspace command, control, communications, computers, and intelligence (C4I) systems for the USG.

g. (~~S~~//~~Rel to USA, AUS, GBR~~) Assumptions.

(1) (~~S~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(2) (~~S~~//~~Rel to USA, AUS, GBR~~) Adversaries are and will (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(3) (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

(4) (~~S~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) adversary's objective

(5) (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

(6) (~~S~~//~~Rel to USA, AUS, GBR~~) Methods will be developed that can  
(b)(1) Sec 1.4(a)

(7) (U) Working relationships will exist with military and civilian Law Enforcement Agencies and Counterintelligence organizations to facilitate identification and apprehension of persons responsible for attacks and/or intrusions on DOD computers and DOD computer networks of the GIG.

(8) (~~S~~) The United States should (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) cyberspace operations.

(9) (U) Planning and conduct of cyberspace operations requires the integration of other elements of national power.

1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819

h. (U) Limitations.

(1) (U) Constraints.

(a) (U) Combatant commands will coordinate their planning with CDRUSSTRATCOM.

(b) (U) CDRUSSTRATCOM will coordinate planning with other combatant commanders.

(c) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(d) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) must be in compliance with US law and DOD Policy.

(2) (~~S//Rel to USA, AUS, GBR~~) Restraint. DOD (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

i. (U) Legal Considerations.

(1) (~~S//Rel to USA, AUS, GBR~~) CONPLAN 8039 contemplates military actions (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

2. (~~S//Rel to USA, AUS, GBR~~) Mission. CDRUSSTRATCOM plans and directs integrated DOD operations in and through cyberspace (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)



1820 3. (U) Execution.

1821

1822 a. Concept of Operations.

1823

1824 (1) (~~S//Rel to USA, AUS, GBR~~) Purpose. The purpose of this plan  
1825 is to provide a framework for cyberspace planning and to  
1826 develop a structure for pre-planned authorities to conduct  
1827 operations in and through cyberspace. Additionally, this plan

1828 (b)(1) Sec 1.4(a)  
1829  
1830

1831

1832 (2) (U) Method. The plan will:

1833

(a) (U) Describe the operation and defense of the GIG.

1834

(b) (U) Provide the context for a common planning structure.

1835

(c) (U) Develop a system of RAs and Cyber Engagement Criteria  
1836 for execution of pre-planned activities and authorities.

1837

(d) (U) Clarify global vs. regional roles and responsibilities and  
1838 lays out coordination methods and instructions.

1839

1840

1841 (3) (~~S//Rel to USA, AUS, GBR~~) End-state. At the end state, the US

1842

1843 (b)(1) Sec 1.4(a)

1844

1845 (b)(1) Sec 1.4(a) Per refs v and x, CONPLAN 8039 will support the  
1846 following termination criterion that support this end-state

1847

1848 (a) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

1849

1850 (b)(1) Sec 1.4(a)

1851

1852

1853 (b) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

1854

1855 (b)(1) Sec 1.4(a)

1856

1857

1858 (c) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

1859

(b)(1) Sec 1.4(a)

1860

1861 (d) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

1862

(b)(1) Sec 1.4(a)

1863

1864 (e) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

1865

(b)(1) Sec 1.4(a)

1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911

(f) (~~S//Rel to USA, AUS, GBR~~) Cyberspace capabilities provide

(b)(1) Sec 1.4(a)

(g) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(h) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(i) (U) Adversaries are deterred from establishing or employing offensive capabilities against US interests in cyberspace.

(j) (U) Adversaries who jeopardize US interests in cyberspace are defeated.

(k) (U) DOD is postured to support homeland security, critical infrastructure protection, and provide civil support.

(l) (U) US, allies, and coalition partners have freedom of action to operate in cyberspace.

b. (~~S//Rel to USA, AUS, GBR~~) General.

(1) (U) Common Context. In order to accomplish its UCP mandated cyberspace mission, outlined in ref e, CONPLAN 8039 establishes a common context with regard to cyberspace domain for military areas of operation and activities. This common context is established through the planning construct and the contents of the Terms of Reference.

(2) (U) Identify Threats and Prioritize Planning Efforts.

(a) (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

plan. Combatant commanders who deviate from the

(b)(1) Sec 1.7(e) will provide rationale to CJCS before developing courses of action.

(b) (~~S//NF~~) The United States information infrastructure is

(b)(1) Sec 1.4(a)

**SECRET**

1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957

(b)(1) Sec 1.4(a)

(c) (S//NF) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) Rapid changes in technology, the integration of telecommunications and computer networks, (b)(1) Sec 1.4(a)

(3) (U) Plan (b)(1) Sec 1.7(e) CONPLAN 8039 will provide the methodology for cyberspace planning (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(U)(a) (S//Rel to USA, AUS, GBR) Actors. Broadly characterized as follows (excerpted and summarized from the National Institute of Standards and Technology (NIST) 800-82):

- 1 (U) National Governments/Foreign Intelligence Services. Characterized by sophisticated, well funded programs to develop cyber tools capable of causing a full spectrum of effects, from propaganda and low-level nuisance web page defacement to pervasive espionage, to widespread, long-duration damage to US critical interests and infrastructures.

**SECRET**

**SECRET**

1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003

- 2 (U) Terrorists. Characterized by a desire to destroy, incapacitate or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the US economy and damage public morale and confidence. Terrorists' cyber efforts are less sophisticated than nation states, but are increasingly dangerous and effective as their technical sophistication increases.
  
- 3 (U) Criminal groups. International organized crime and industrial espionage is less directly threatening to US security interests due to a focus on profit motive. Nonetheless, this category of actors presents a threat due to their ability to hire, develop and retain sophisticated talent and tools.
  
- 4 (U) Hacktivists. Hacktivists form a small, foreign population of politically active hackers that includes individuals and groups with anti-US motives. They pose a medium-level threat of carrying out an isolated but damaging attack. Most hacktivist groups appear bent on propaganda rather than damage to critical infrastructures. Their primary goal is to support political agendas with sub-goals of propaganda and causing damage to achieve notoriety for their cause.
  
- 5 (U) Hackers. This category includes a wide variety of sub-categories, including Phishers, Spammers, Spyware/Malware Authors, Script Kiddies and professional Black Hats. In general the large majority of hackers do not have sufficient talent to threaten difficult targets such as critical US and defense systems. Nonetheless, the large global population of hackers poses a relatively high threat of disruptions in a variety of networks and systems, with potential for property damage and loss of life. As the hacker population grows, so does the likelihood of an exceptionally skilled, lucky or malicious hacker attempting and succeeding in an extremely damaging attack.

(b) (~~S//Rel to USA, AUS, GBR~~) Scenarios. (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) CONPLAN 8039 will draw upon  
the following to (b)(1) Sec 1.4(a) specific  
scenarios:

**SECRET**

2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049

1 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
ref v (e.g. planning support to applicable USSTRATCOM  
CONPLANS/OPLANS, (b)(1) Sec 1.4(a)  
etc.).

2 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(c) (U) Objectives and (b)(1) Sec 1.7(e)

1 (U) For the purposes of this plan, CONPLAN 8039 will  
use the following (b)(1) Sec 1.7(e)  
derived from refs c, e, h, v and x.

a (~~S~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) This also includes  
coordination with (b)(1) Sec 1.4(a) and the  
(b)(1) Sec 1.4(a)  
in securing US cyberspace in support of the respective  
Combatant Commanders.

b (~~S~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

c (~~S~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

2 (U) CONPLAN 8039 will support objectives and (b)(1) Sec 1.7(e)  
operations based on:

a (~~S//Rel to USA, AUS, GBR~~) When CDRUSSTRATCOM  
is the supported commander in response to a cyber  
threat, CONPLAN 8039 will provide the means to  
(b)(1) Sec 1.4(a)

2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087

b (~~S//Rel to USA, AUS, GBR~~) When CDRUSSTRATCOM is the supported commander for operations in and through cyberspace (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) cyber effects will be based on (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

c (~~S//Rel to USA, AUS, GBR~~) When CDRUSSTRATCOM is supporting commander to other Combatant Commanders, (b)(1) Sec 1.4(a) will provide supporting cyber effects based (b)(1) Sec 1.4(a) CONPLAN 8039. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) This also includes coordination (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) For timing and tempo of operations, USSTRATCOM assigned cyber forces will follow the supported commander or agency's (b)(1) Sec 1.4(a) or planned construct.

d (~~S//Rel to USA, AUS, GBR~~) In order to successfully execute operations in and through cyberspace supported combatant commanders (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (objectives), and the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

- (b)(1) Sec 1.7(e)
  - 1.0 (U) (b)(1) Sec 1.7(e)
  - 2.0 (U)
  - 3.0 (U)
- (b)(1) Sec 1.7(e)
  - 1.1 (U) U.S. (b)(1) Sec 1.7(e)
  - 1.2 (U) U.S.
  - 1.3 (U) U.S.
  - 1.4 (U) U.S.
  - 1.5 (U) U.S.
  - 1.6 (U) U.S.
- (b)(1) Sec 1.7(e)
  - 2.1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
  - 2.2 (S//Rel to USA, AUS, GBR)
  - 2.3 (S//Rel to USA, AUS, GBR)
  - 2.4 (S//Rel to USA, AUS, GBR)
  - 2.5 (S//Rel to USA, AUS, GBR)
  - 2.6 (S//Rel to USA, AUS, GBR)
- (b)(1) Sec 1.7(e)
  - 3.1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)
  - 3.2 (S//Rel to USA, AUS, GBR)
  - 3.3 (S//Rel to USA, AUS, GBR)
  - 3.4 (S//Rel to USA, AUS, GBR)
  - 3.5 (S//Rel to USA, AUS, GBR)
  - 3.6 (S//Rel to USA, AUS, GBR)
- Action (Example)**  
 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

**Capabilities**  
 (U) Attack adversary critical vulnerabilities in cyberspace  
 (U) Defend critical vulnerabilities through implementation of cyberspace defense-in-depth measures

**Supporting Key Capabilities POCs**  
 (U) JFCC NW, JTF GNO, JIOWC, JFCC GSI

**Network Elements**  
 (U) Electromagnetic Spectrum, Infrastructure, Data, Purpose

Figure 7: (S//Rel to USA, AUS, GBR) Synopsis of key CONPLAN 8039 execution concepts

2088  
 2089  
 2090  
 2091  
 2092  
 2093  
 2094  
 2095  
 2096  
 2097  
 2098  
 2099  
 2100  
 2101

(1) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) planners will consider

(b)(1) Sec 1.4(a)

**SECRET**

2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147

(2) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
When planning in support of other plans, planners  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) as defined in ref O.

(3) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) When  
(b)(1) Sec 1.4(a)

e (U) Per ref bi, the supported commander plans joint operations based on analysis of national strategic objectives and development of theater objectives supported by (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

(d) (U) Planning.

1 (~~S//Rel to USA, AUS, GBR~~) Planning will consider all  
(b)(1) Sec 1.4(a) and  
COA development. (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) Specific mission  
analysis and COA development will (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
Further information on (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) and COA  
development can be found in Annex C and (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

2 (~~S//Rel to USA, AUS, GBR~~) Upon request for CONPLAN 8039 support, USSTRATCOM will collaborate with  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) commands  
/services/agencies (C/S/As) should be included in the planning process for coordination and deconfliction.

3 (~~S//Rel to USA, AUS, GBR~~) USSTRATCOM may request  
(b)(1) Sec 1.4(a)



**SECRET**

2148  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2170  
2171  
2172  
2173  
2174

(b)(1) Sec 1.4(a) to support objectives. In instances where another CCDR supported CDRUSSTRATCOM will facilitate this coordination. USSTRATCOM will work with the Office of the Secretary of Defense (OSD) and Joint Staff to garner (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

4 (S//~~Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) and will be approved via the EXORD that authorizes the supported operation or a separate EXORD, if needed. The criteria (b)(1) Sec 1.4(a) (see Figure 8, below) will be dependent upon:

(b)(1) Sec 1.4(a)

Figure 8: (S//~~Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

\*Note 1: (b)(1) Sec 1.4(a) can be found in the Terms of Reference.

\*Note 2: Authorities listed are only exemplary in nature. Any (b)(1) Sec 1.4(a)

\*Note 3: Large X indicates (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) A need to use

**SECRET**

**SECRET**

(b)(1) Sec 1.4(a)

2175  
2176  
2177  
2178  
2179  
2180  
2181  
2182  
2183  
2184  
2185  
2186  
2187  
2188  
2189  
2190  
2191  
2192  
2193  
2194  
2195  
2196  
2197  
2198  
2199  
2200  
2201  
2202  
2203  
2204  
2205  
2206  
2207  
2208  
2209  
2210  
2211  
2212  
2213  
2214  
2215  
2216  
2217  
2218  
2219

a (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) A more

(b)(1) Sec 1.4(a)

The planning effort must address the need for (b)(1) Sec 1.4(a) that supports the access development of desired (b)(1) Sec 1.4(a)

b (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) will not normally require (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

c (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) see Terms of Reference.

These definitions will be used when making a (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) within the purview of CONPLAN 8039. The probable (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

d (U) Authorities: The level of authority is generally

(b)(1) Sec 1.7(e)

engagement criteria; (b)(1) Sec 1.7(e) will normally

be associated with (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) Independent of the scale of the

2220  
2221  
2222  
2223  
2224  
2225  
2226  
2227  
2228  
2229  
2230  
2231  
2232  
2233  
2234  
2235  
2236  
2237  
2238  
2239  
2240  
2241  
2242  
2243  
2244  
2245  
2246  
2247  
2248  
2249  
2250  
2251  
2252  
2253  
2254  
2255  
2256  
2257  
2258  
2259  
2260  
2261  
2262  
2263  
2264  
2265

cyber engagement criteria, (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

e (~~S//Rel to USA, AUS, GBR~~) The engagement criteria  
which encompasses the (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) will be delineated in  
the applicable EXORD. Within that EXORD, (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(4) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) CONPLAN 8039 will (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) in support of assigned objectives.

(a) (U) General.

1 (~~S//Rel~~) Upon plan approval and appropriate authorities  
granted via EXORD, CONPLAN 8039 will be used to (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) Operations will be coordinated with  
Combatant Commanders during the planning and  
execution phase to mitigate AOR/functional mission (s)  
impact.

2 (~~S//Rel~~) On order, CONPLAN 8039 will (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) and other numbered plans.

(b) (~~FOUO~~) Cyberspace desired effects.

1 (~~FOUO~~) (b)(1) Sec 1.7(e) This plan will define the range of  
effects in cyberspace by using (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) (see Terms of Reference).

2 (~~S//REL TO USA, AUS, GBR~~) To assist planners in  
building (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) (see Terms of  
Reference). (b)(1) Sec 1.4(a)

**SECRET**

2266  
2267  
2268  
2269  
2270  
2271  
2272  
2273  
2274  
2275  
2276  
2277  
2278  
2279  
2280  
2281  
2282  
2283  
2284  
2285  
2286  
2287  
2288  
2289  
2290  
2291  
2292  
2293  
2294  
2295  
2296  
2297  
2298  
2299  
2300  
2301  
2302  
2303  
2304  
2305  
2306  
2307  
2308  
2309  
2310  
2311

(b)(1) Sec 1.4(a) before a JFC must seek additional authorities. CONPLAN 8039 will use them as one of the components of the (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) available to the JFC, but only by receiving specific permission from the (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(c) (U) (b)(1) Sec 1.7(e) in cyberspace. In order to (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) in cyberspace, USSTRATCOM (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) These capabilities are all employed in support of the JFC.

1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) CONPLAN 8039 recognizes there are (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) For prospective supported and supporting commands, USSTRATCOM has assigned component focal points for the (b)(1) Sec 1.4(a) in and through cyberspace. In each case, (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Specific details outlining these supporting concepts and how each USSTRATCOM component (b)(1) Sec 1.4(a) CONPLAN 8039 can be found in Annex C.

2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) This is accomplished by comparing the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

2312  
2313  
2314  
2315  
2316  
2317  
2318  
2319  
2320  
2321  
2322  
2323  
2324  
2325  
2326  
2327  
2328  
2329  
2330  
2331  
2332  
2333  
2334  
2335  
2336  
2337  
2338  
2339  
2340  
2341  
2342  
2343  
2344  
2345  
2346  
2347  
2348  
2349  
2350  
2351  
2352  
2353  
2354  
2355  
2356  
2357

(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) should be viewed as a way to  
(b)(1) Sec 1.4(a)  
planner must first understand the (b)(1) Sec 1.4(a) and then  
(b)(1) Sec 1.4(a)

3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
Planners should recommend the (b)(1) Sec 1.4(a)  
types that (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) Commanders should ensure that these (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) In some cases, it may be  
necessary to (b)(1) Sec 1.4(a)  
to achieve the commander's objective. Again, it is  
important to emphasize that (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(5) (U) Operations. As in the physical domains (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) discussion and terminology can be  
found in the Terms of Reference. This need for increasing  
(b)(1) Sec 1.7(e)  
usually require supplemental ROE (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) Exemplar supplemental ROE (b)(1) Sec 1.7(e)  
(outside of ref o) are detailed in Annex J. Example  
supplemental ROE for (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

(a) (U) Supporting Command. USSTRATCOM will normally  
(b)(1) Sec 1.7(e) as the supporting commander to other  
CCDRs. USSTRATCOM will follow the (b)(1) Sec 1.7(e)  
construct defined by the supported commander or activity  
and employ cyber forces and execute operations in support  
of plan objectives. General discussion on USSTRATCOM  
cyberspace support is found in applicable USSTRATCOM  
supporting CONPLANS. More detailed handling of these  
activities will be captured in Annex C, (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

**SECRET**

2358  
2359  
2360  
2361  
2362  
2363  
2364  
2365  
2366  
2367  
2368  
2369  
2370  
2371  
2372  
2373  
2374  
2375  
2376  
2377  
2378  
2379  
2380  
2381  
2382  
2383  
2384  
2385  
2386  
2387  
2388  
2389  
2390  
2391  
2392  
2393  
2394  
2395  
2396  
2397  
2398  
2399  
2400  
2401  
2402  
2403

(b) (U) Supported Command. When CDRUSSTRATCOM is designated the supported commander against cyber threat actors, CONPLAN 8039 will use the (b)(1) Sec 1.7(e) outlined in ref bi. See (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) but the process is situation dependent, and commanders have the flexibility to employ or recommend any appropriate, approved responses at any time.

(c) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) allows military commanders to develop (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

1 (~~S//Rel to USA, AUS, GBR~~) Process. Typically (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) If existing accesses to the (b)(1) Sec 1.4(a) are sufficient to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

2 (~~S//Rel to USA, AUS, GBR~~) Risk Relationship. When considering requesting or authorizing (b)(1) Sec 1.4(a) commanders should balance the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) relationship between (b)(1) Sec 1.4(a) commanders should consider (b)(1) Sec 1.4(a)

3 (~~S//Rel to USA, AUS, GBR~~) Authorities. IAW ref o, the authority to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) generally granted through an EXORD. When CDRUSSTRATCOM is the supported commander this authority maybe delegated to the JFCC NW Commander.

**SECRET**

2404  
2405  
2406  
2407  
2408  
2409  
2410  
2411  
2412  
2413  
2414

Further discussion of (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(d) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) See Figure 9,  
below, for a summary of (b)(1) Sec 1.4(a)  
discussed below. Each of the (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

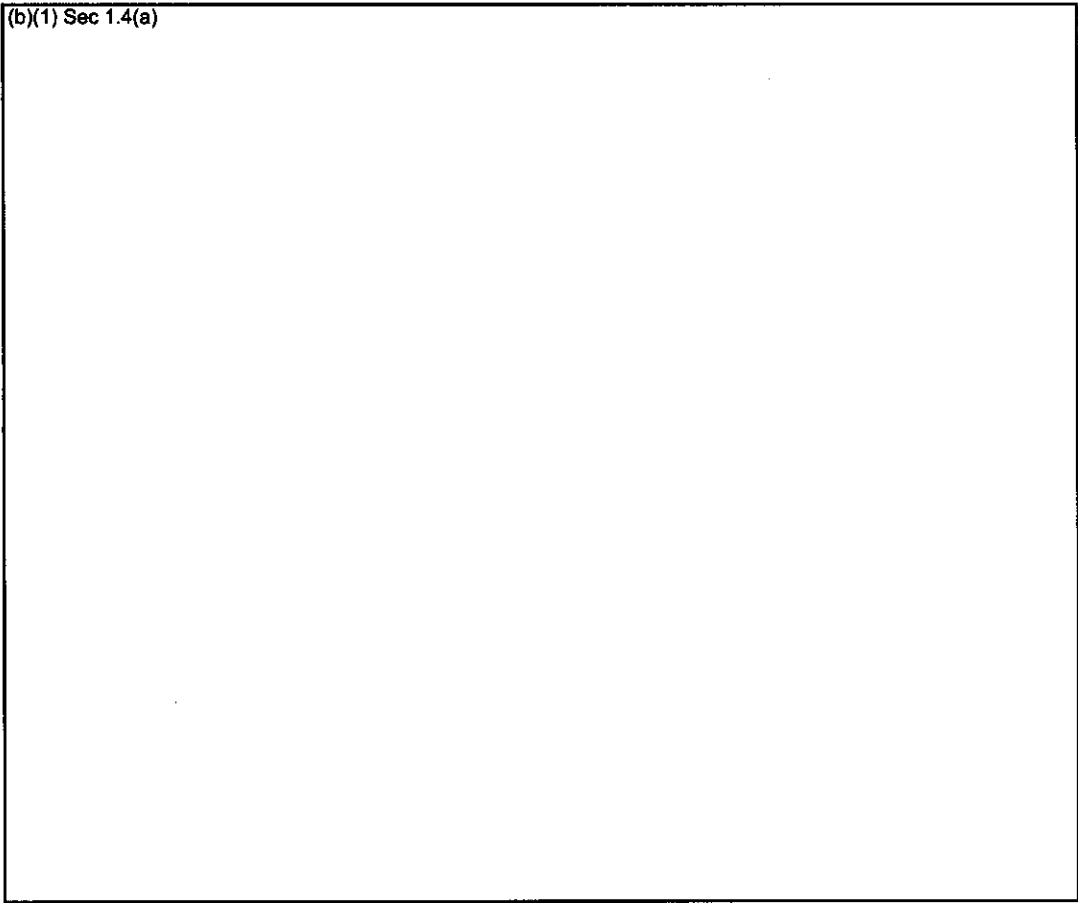


Figure 9 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(EXAMPLE)

2415  
2416  
2417  
2418  
2419  
2420  
2421

(e) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
1 (~~S//Rel to USA, AUS, GBR~~) Commander's Intent.  
Support US government efforts to (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

**SECRET**

2422  
2423  
2424  
2425  
2426  
2427  
2428  
2429  
2430  
2431  
2432  
2433  
2434  
2435  
2436  
2437  
2438  
2439  
2440  
2441  
2442  
2443  
2444  
2445  
2446

(b)(1) Sec 1.4(a)

2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

cooperation, even within the context of the cyberspace mission area. (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) The JFC will consider

(b)(1) Sec 1.4(a)

3 (U) (b)(1) Sec 1.7(e) The following are general (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)



(b)(1) Sec 1.7(e)

2.1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.1.1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.1.2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.1.3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.2.1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.2.2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.2.3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.3.1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.3.2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.3.3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.4 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.4.1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.4.2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.4.3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2.5 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 2.5.1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 2.5.2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 2.5.3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 2.6 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 2.6.1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 2.6.2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 2.6.3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.7(e)  
 3.1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 3.2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 3.3 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 3.4 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 3.5 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 3.6 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)

Figure 10: (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)

2447  
 2448  
 2449  
 2450  
 2451  
 2452  
 2453  
 2454  
 2455  
 2456  
 2457  
 2458  
 2459  
 2460  
 2461  
 2462

4 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)

a (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)  
 Normally, the JFC (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a) operations. Therefore, special circumstance  
 and authorities in (b)(1) Sec 1.4(a)  
 (b)(1) Sec 1.4(a)

2463  
2464  
2465  
2466  
2467  
2468  
2469  
2470  
2471  
2472  
2473  
2474  
2475  
2476  
2477  
2478  
2479  
2480  
2481  
2482  
2483  
2484  
2485  
2486  
2487  
2488  
2489  
2490  
2491  
2492  
2493  
2494  
2495  
2496  
2497  
2498  
2499  
2500  
2501  
2502  
2503  
2504  
2505  
2506  
2507

b (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
accomplishment. In order to (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) the JFC is normally (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

c (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

5 (U) Execution. Specific details on how cyber forces will  
execute their mission will be covered in Annex C and in  
(b)(1) Sec 1.7(e)

a (U) (b)(1) Sec 1.7(e)  
Execution activities are identified.

b (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) These are activities that are  
accomplished (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

c (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

d (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

2508  
2509  
2510  
2511  
2512  
2513  
2514  
2515  
2516  
2517  
2518  
2519  
2520  
2521  
2522  
2523  
2524  
2525  
2526  
2527  
2528  
2529  
2530  
2531  
2532  
2533  
2534  
2535  
2536  
2537  
2538  
2539  
2540  
2541  
2542  
2543  
2544  
2545  
2546  
2547  
2548  
2549  
2550  
2551  
2552  
2553

6 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
Cyber forces will (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) Also, other domain-specific (b)(1) Sec 1.4(a) operations in and through cyberspace. Specific details on how cyber forces (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

a (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) As the cyber campaign progresses, the supported JFC must (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
Refer to the Executive Summary (b)(1) Sec 1.4(a) and (b)(1) Sec 1.4(a)

b (U) (b)(1) Sec 1.7(e)

(1) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Unlike (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) the JFC can prioritize defense readiness based on likely (b)(1) Sec 1.4(a) In addition, the JFC can (b)(1) Sec 1.4(a) based on increased operational requirements for US cyberspace to function. A method to describe this is the (b)(1) Sec 1.4(a).

(2) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) See Figure 8, above to describe (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(3) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) USSTRATCOM may use (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

2554  
2555  
2556  
2557  
2558  
2559  
2560  
2561  
2562  
2563  
2564  
2565  
2566  
2567  
2568  
2569  
2570  
2571  
2572  
2573  
2574  
2575  
2576  
2577  
2578  
2579  
2580  
2581  
2582  
2583  
2584  
2585  
2586  
2587  
2588  
2589  
2590  
2591  
2592  
2593  
2594  
2595  
2596  
2597  
2598  
2599

7 ~~(S//Rel to USA, AUS, GBR)~~ (b)(1) Sec 1.4(a) Specific details on how (b)(1) Sec 1.4(a) will be covered in Annex C and (b)(1) Sec 1.4(a) As outlined above, CDRUSSTRATCOM can be the designated supported or supporting commander for operations in and through cyberspace. (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

a ~~(S//Rel to USA, AUS, GBR)~~ Supported Commander. As the supported commander, CDRUSSTRATCOM will:

(1) ~~(S//Rel to USA, AUS, GBR)~~ Determine (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

attain the objective.

(2) ~~(S//Rel to USA, AUS, GBR)~~ Highlight the

(b)(1) Sec 1.4(a)

(3) ~~(FOUO)~~ Determine (b)(1) Sec 1.7(e) o emphasize the desired end-state. Some cyberspace

(b)(1) Sec 1.7(e)

(4) ~~(FOUO)~~ Provide guidance on his objectives, desired

(b)(1) Sec 1.7(e)

b (U) Supporting Commander. As the supporting commander, CDRUSSTRATCOM will assist the supported JFC to accomplish the above tasks from a cyberspace perspective as required. General discussion on USSTRATCOM cyberspace support is found in applicable USSTRATCOM supporting CONPLANS. Specific details on USSTRATCOM cyberspace operational support will be provided in

(b)(1) Sec 1.7(e)

(f) ~~(S//Rel to USA, AUS, GBR)~~ (b)(1) Sec 1.4(a)

2600  
2601  
2602  
2603  
2604  
2605  
2606  
2607  
2608  
2609  
2610  
2611  
2612  
2613  
2614  
2615  
2616  
2617  
2618  
2619  
2620  
2621  
2622  
2623  
2624  
2625  
2626  
2627  
2628  
2629  
2630  
2631  
2632  
2633  
2634  
2635  
2636  
2637  
2638  
2639  
2640  
2641  
2642  
2643  
2644  
2645

1 (U) Commander's Intent. (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) establish/maintain  
normal operations of the DOD GIG, (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

2 (U) (b)(1) Sec 1.7(e) operations are characterized by  
(b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) phase in that it is  
largely characterized by (b)(1) Sec 1.7(e)  
specifically support (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

3 (U) Objectives (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) That sections lists general  
operational (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)  
support the (b)(1) Sec 1.7(e)  
action in cyberspace and support to other operations  
through cyberspace will be covered in (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

4 (~~S~~//Rel to USA, AUS, GBR) Risk.  
a (~~S~~//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) Normally  
the JFC is (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) Therefore, special circumstance and  
authorities in (b)(1) Sec 1.4(a) must be provided in order to  
(b)(1) Sec 1.4(a)  
b (~~S~~//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

**SECRET**

2646  
2647  
2648  
2649  
2650  
2651  
2652  
2653  
2654  
2655  
2656  
2657  
2658  
2659  
2660  
2661  
2662  
2663  
2664  
2665  
2666  
2667  
2668  
2669  
2670  
2671  
2672  
2673  
2674  
2675  
2676  
2677  
2678  
2679  
2680  
2681  
2682  
2683  
2684  
2685  
2686  
2687  
2688  
2689  
2690  
2691

(b)(1) Sec 1.4(a)

c ~~c~~ (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

5 (U) Execution. See (b)(1) Sec 1.7(e) above.

6 ~~(S//Rel to USA, AUS, GBR)~~ (b)(1) Sec 1.4(a) See  
(b)(1) Sec 1.4(a) above.

7 ~~(S//Rel to USA, AUS, GBR)~~ (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) The cyberspace planner should  
consider (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) when crafting  
options for the commander.

(g) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

1 ~~(S//Rel to USA, AUS, GBR)~~ Commander's Intent. Prepare  
(b)(1) Sec 1.4(a)

2 (U) Timing. (b)(1) Sec 1.7(e) operations in and through  
cyberspace (b)(1) Sec 1.7(e)  
to expand friendly freedom of action in cyberspace  
continue while the JFC (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) with the intent  
of resolving the crisis at the earliest opportunity. The  
supported JFC (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

**SECRET**

2692  
2693  
2694  
2695  
2696  
2697  
2698  
2699  
2700  
2701  
2702  
2703  
2704  
2705  
2706  
2707  
2708  
2709  
2710  
2711  
2712  
2713  
2714  
2715  
2716  
2717  
2718  
2719  
2720  
2721  
2722  
2723  
2724  
2725  
2726  
2727  
2728  
2729  
2730  
2731  
2732  
2733  
2734  
2735  
2736  
2737

across/through the DOD GIG. (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

3 (U) Objectives and (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

4 (S//Rel to USA, AUS, GBR) Risk.

a (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
Normally the JFC will consider taking (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

b (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) The JFC is normally focused on  
(b)(1) Sec 1.4(a)

c (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
The JFC will consider using (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) and will be less concerned with  
(b)(1) Sec 1.4(a)

5 (U) Execution. See (b)(1) Sec 1.7(e)

6 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) See  
(b)(1) Sec 1.4(a)

7 (S//Rel USA, AUS, GBR) (b)(1) Sec 1.4(a)  
operations (b)(1) Sec 1.4(a) The  
cyberspace planner must consider (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) if attributed in  
(b)(1) Sec 1.4(a) when crafting options for the commander.

(h) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

1 (U) Commander's Intent. (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)



**SECRET**

2738  
2739  
2740  
2741  
2742  
2743  
2744  
2745  
2746  
2747  
2748  
2749  
2750  
2751  
2752  
2753  
2754  
2755  
2756  
2757  
2758  
2759  
2760  
2761  
2762  
2763  
2764  
2765  
2766  
2767  
2768  
2769  
2770  
2771  
2772  
2773  
2774  
2775  
2776  
2777  
2778  
2779  
2780  
2781  
2782  
2783

cyberspace. In addition, USSTRATCOM may be called upon to

(b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

2 (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

JFC will not normally

(b)(1) Sec 1.7(e) The supported JFC will consider progressing to

(b)(1) Sec 1.7(e)

3 (U) Objectives and (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

4 (S//Rel to USA, AUS, GBR) Risk.

a (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

b (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

c (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

**SECRET**

2784  
2785  
2786  
2787  
2788  
2789  
2790  
2791  
2792  
2793  
2794  
2795  
2796  
2797  
2798  
2799  
2800  
2801  
2802  
2803  
2804  
2805  
2806  
2807  
2808  
2809  
2810  
2811  
2812  
2813  
2814  
2815  
2816  
2817  
2818  
2819  
2820  
2821  
2822  
2823  
2824  
2825  
2826  
2827  
2828  
2829

5 (U) Execution. See (b)(1) Sec 1.7(e)

6 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) See (b)(1) Sec 1.4(a)

7 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(i) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

1 (U) Commander's Intent. (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

2 (U) Timing. The (b)(1) Sec 1.7(e) is typically characterized by a change (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) to ensure that the situation leading to the original crisis does not reoccur and/or its effects are mitigated. Throughout this segment, the JFC continuously assesses the impact of current cyberspace operations (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

3 (U) Objectives and (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

4 (U) Risk.

a (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) Normally

2830  
2831  
2832  
2833  
2834  
2835  
2836  
2837  
2838  
2839  
2840  
2841  
2842  
2843  
2844  
2845  
2846  
2847  
2848  
2849  
2850  
2851  
2852  
2853  
2854  
2855  
2856  
2857  
2858  
2859  
2860  
2861  
2862  
2863  
2864  
2865  
2866  
2867  
2868  
2869  
2870  
2871  
2872  
2873  
2874

the JFC is (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

b (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) In order to limit (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) the JFC is normally more focused  
(b)(1) Sec 1.4(a)

c (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
In order to minimize (b)(1) Sec 1.4(a) in  
(b)(1) Sec 1.4(a)

5 (U) Execution. See (b)(1) Sec 1.7(e)

6 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) See  
(b)(1) Sec 1.4(a)

7 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
operations (b)(1) Sec 1.4(a) The planner  
must consider the (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(j) (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)

1 (U) Commander's Intent. Provide support, as applicable  
(b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) of cyberspace systems and/or  
infrastructure, as directed.

2 (U) Timing. (b)(1) Sec 1.7(e) is predominately characterized by  
cyberspace (b)(1) Sec 1.7(e) The  
goal is for cyberspace forces to (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

2875  
2876  
2877  
2878  
2879  
2880  
2881  
2882  
2883  
2884  
2885  
2886  
2887  
2888  
2889  
2890  
2891  
2892  
2893  
2894  
2895  
2896  
2897  
2898  
2899  
2900  
2901  
2902  
2903  
2904  
2905  
2906  
2907  
2908  
2909  
2910  
2911  
2912  
2913  
2914  
2915  
2916  
2917  
2918  
2919  
2920

(b)(1) Sec 1.7(e)

3 (U) Objectives and (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

4 (U) Risk.

a (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

b (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) In order to (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) the JFC is normally more focused  
on (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

c (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
In order to minimize (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

5 (U) Execution. See (b)(1) Sec 1.7(e)

6 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a) See  
(b)(1) Sec 1.4(a)

7 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) The  
cyberspace planner must consider (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

c. c. (U) Tasks.

(1) HQ USSTRATCOM.

(a) (U) Provide Commander's Intent by developing Operations Orders (OPORDs) and Execution Orders (EXORDs) to

**SECRET**

- 2921 support strategic/global DOD cyberspace operations, as  
2922 necessary.  
2923
- 2924 (b) (U) Provide an updated Commander's Intent with regard to  
2925 cyberspace operations prior to execution of operations and  
2926 (b)(1) Sec 1.7(e)  
2927
- 2928 (c) (U) Ensure C/S/As' contingency and crisis plans for CO are  
2929 integrated and coordinated across the DOD GIG.  
2930
- 2931 (d) (U) Sponsor DOD-wide development of CO crisis action  
2932 plans, policies, and doctrine in order to support and  
2933 (b)(1) Sec 1.7(e)  
2934
- 2935 (e) (~~S//Rel to USA, AUS, GBR~~) Develop strategic-level plans to  
2936 (b)(1) Sec 1.4(a)  
2937  
2938  
2939  
2940
- 2941 (f) (U) Advise and coordinate with supporting and supported  
2942 commander on matters concerning the employment and  
2943 limitations (e.g., logistics) of such support, assist in planning  
2944 for the integration of such support into the supported  
2945 commander's effort as a whole, and ensure that support  
2946 requirements are appropriately communicated within  
2947 USSTRATCOM.  
2948
- 2949 (g) (U) Coordinate with combatant commanders to review and  
2950 update their prioritization assessment for defense and  
2951 reconstitution of their networks. Assessments shall identify  
2952 current mission-critical, mission-essential, and mission-  
2953 support networks.  
2954
- 2955 (h) (~~S//Rel to USA, AUS, GBR~~) Per ref c, coordinate planning  
2956 with other combatant commanders, to include assisting  
2957 combatant commanders (b)(1) Sec 1.4(a)  
2958 (b)(1) Sec 1.4(a)  
2959  
2960  
2961
- 2962 (i) (U) Support and coordinate CO information sharing with  
2963 alliance and coalition partners concerning any ambiguous  
2964 emerging threats based on guidance provided in the  
2965 approved Delegation of Disclosure Letter (ref k) and  
2966 applicable Memoranda of Agreement/Memoranda of

**SECRET**

**SECRET**

- 2967 Understanding (MOA/MOU). Coordination and agreements  
2968 will be IAW CJCSI 2300.01A and CJCSI 5130.01A.  
2969 Disclosure of classified information will be IAW CJCSI  
2970 5221.01A.  
2971  
2972 (j) (U) Maintain liaison with appropriate government agencies,  
2973 with OSD and Joint Staff oversight, for CO and COA  
2974 development.  
2975  
2976 (k) (U) Based on guidance provided in approved information  
2977 releasability policies and procedures, support and advocate  
2978 increased information sharing with the private sector.  
2979  
2980 (l) (U) Per ref j, and Annex C, conduct Computer Network  
2981 Assessment Conferences (NACs):  
2982  
2983 1 (U) Prior to execution of CONPLAN 8039.  
2984  
2985 2 (U) Prior to changing phases when not preempted by pre-  
2986 planned responses.  
2987  
2988 3 (U) Prior to providing recommendations for the use of the  
2989 elements of national power in cyberspace operations to  
2990 SECDEF.  
2991  
2992 4 (U) Prior to developing conventional and special  
2993 operations, CO and other IO COAs.  
2994  
2995 (m) (U) Communicate to the DOD Chief Information  
2996 Officer (CIO) the level of agility and responsiveness of the  
2997 DOD GIG to conduct CO. USSTRATCOM shall also identify  
2998 to the DOD CIO threats to the DOD GIG. DOD CIO has legal  
2999 responsibility under the Clinger-Cohen Act of 1996 to  
3000 acquire architectural and configuration control over the DOD  
3001 portion of the DOD GIG.  
3002  
3003 (n) (U) Reference COOP IAW ref bl in order to conduct  
3004 operations when the ability to access the DOD GIG is denied.  
3005  
3006 (o) (~~S//Rel to USA, AUS, GBR~~) Identify desired (b)(1) Sec 1.4(a)  
3007 (b)(1) Sec 1.4(a)  
3008  
3009 (b)(1) Sec 1.4(a) in support  
3010 of other combatant commanders as directed.  
3011

**SECRET**

**SECRET**

- 3012 (p) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) and
- 3013 coordinate approval with SECDEF and C/S/As, as required.
- 3014
- 3015 (q) (U) Exercise command and control of selected missions, as
- 3016 directed.
- 3017
- 3018 (r) (U) Assess the operational impact of recommended CO
- 3019 response actions.
- 3020
- 3021 (s) (U) Gather, analyze and report at the strategic level, combat
- 3022 assessment information necessary for continued
- 3023 defending/defeating operations.
- 3024
- 3025 (t) (U) As approved by the Secretary of Defense (b)(1) Sec 1.7(e)
- 3026 (b)(1) Sec 1.7(e) as necessary.
- 3027
- 3028 (u) (U) Provide technical, planning and/or operational offensive
- 3029 cyber-related advice and, upon request, actions to contain
- 3030 (b)(1) Sec 1.7(e)
- 3031 (b)(1) Sec 1.7(e) in their AORs.
- 3032
- 3033 (v) (~~S//Rel to USA, AUS, GBR~~) Identify and request (b)(1) Sec 1.4(a)
- 3034 (b)(1) Sec 1.4(a)
- 3035 (b)(1) Sec 1.4(a) with respect to cyberspace.
- 3036
- 3037 (w) (~~S//Rel to USA, AUS, GBR~~) Identify and request (b)(1) Sec 1.4(a)
- 3038 (b)(1) Sec 1.4(a)
- 3039
- 3040
- 3041
- 3042 (x) (~~S//Rel to USA, AUS, GBR~~) Request from the (b)(1) Sec 1.4(a)
- 3043 (b)(1) Sec 1.4(a)
- 3044
- 3045
- 3046
- 3047 (y) (~~S//Rel to USA, AUS, GBR~~) Develop and maintain
- 3048 (b)(1) Sec 1.4(a)
- 3049
- 3050
- 3051
- 3052 cyberspace forces and activities.
- 3053
- 3054 (z) (U) Maintain network defense baseline for the DOD GIG.
- 3055
- 3056 (aa) (~~S//Rel to USA, AUS, GBR~~) Disseminate to C/S/As
- 3057 (b)(1) Sec 1.4(a)

**SECRET**

**SECRET**

3058  
3059  
3060  
3061  
3062  
3063  
3064  
3065  
3066  
3067  
3068  
3069  
3070  
3071  
3072  
3073  
3074  
3075  
3076  
3077  
3078  
3079  
3080  
3081  
3082  
3083  
3084  
3085  
3086  
3087  
3088  
3089  
3090  
3091  
3092  
3093  
3094  
3095  
3096  
3097  
3098  
3099  
3100  
3101  
3102  
3103

(b)(1) Sec 1.4(a)

(bb) (U) (~~S//Rel to USA, AUS, GBR~~) As needed, develop and request supplemental ROE from the SECDEF.

(cc) (~~S//Rel to USA, AUS, GBR~~) Plan, coordinate and  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) when directed.

(dd) (~~S//Rel to USA, AUS, GBR~~) Continue and/or expand  
the (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(ee) (~~S//Rel to USA, AUS, GBR~~) Develop and coordinate  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) Based on assessment and recommendation from  
Joint Task Force - Global Network Operations (JTF-GNO).

(ff) (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(gg) (U) Coordinate enhanced information sharing with allies, coalition partners and the private sector, based on approved Delegation of Disclosure Authority Official memorandum (ref 1) and approved MOAs/MOUs. USSTRATCOM HQ/J4 is the OPR for all MOAs/MOUs.

(2) (U) USSTRATCOM Components when directed will:

(a) (U) Recommend changes to daily operations network configurations as a result of lessons learned.

(b) (U) Reference respective component (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

(c) (U) Coordinate with HQ USSTRATCOM on matters pertaining to CO. Implement DOD-wide CO directions from CDRUSSTRATCOM for applicable networks.



**SECRET**

- 3104 (d) ~~(FOUO)~~ Direct and monitor compliance (including CTOs  
3105 (Communications Tasking Order), IAVAs (Information  
3106 Assurance Vulnerability Alerts), and INFOCON (Information  
3107 Operations Condition)) of indigenous networks with approved  
3108 DOD policies and procedures that regulate operations in the  
3109 DOD GIG (see Annex C Operations) and report as required.  
3110
- 3111 (e) ~~(FOUO)~~ Coordinate, execute and/or direct support  
3112 troubleshooting and restoration actions for internal networks  
3113 and systems as required.  
3114
- 3115 (f) ~~(FOUO)~~ Monitor named areas of interests (NAIs) in support  
3116 of JTF-GNO to detect threat activity against the DOD GIG  
3117 (see Annex C, Operations).  
3118
- 3119 (g) ~~(FOUO)~~ Implement response actions in support by JTF-GNO  
3120 (IAW SROE), to correct faults, defeat threat activity, and  
3121 deliver priority information across the DOD GIG (see Annex  
3122 C, Operations).  
3123
- 3124 (h) ~~(FOUO)~~ Implement contingency operations in support of  
3125 JTF-GNO to restore capability and strengthen the DOD GIG  
3126 against further faults, threats and information gaps across  
3127 the DOD GIG (see Annex C, Operations).  
3128
- 3129 (i) ~~(FOUO)~~ Report to JTF-GNO status of internal worldwide  
3130 terrestrial, space and wireless transmission systems and  
3131 enterprise services, and facilities.  
3132
- 3133 (j) ~~(FOUO)~~ Establish, in support of JTF-GNO, procedures for  
3134 dissemination of network operations (NETOPS) related  
3135 advisories, alerts, and warning notices.  
3136
- 3137 (k) ~~(FOUO)~~ Conduct nodal analysis of internal networks to  
3138 determine Critical Nodes, provide this information, and  
3139 assist JTF-GNO and HQ USSTRATCOM with defense and/or  
3140 recovery/restoration operations as required.  
3141
- 3142 (l) (U) Provide recommendations to HQ USSTRATCOM for  
3143 policy, planning, ROE, COAs, INFOCON changes,  
3144 requirements, and mission tactics, techniques and  
3145 procedures (TTPs).  
3146
- 3147 (m) (U) Operations will be coordinated with Combatant  
3148 Commanders during the planning and execution phase to  
3149 mitigate AOI/functional mission (s) impact.

**SECRET**

**SECRET**

3150  
3151  
3152  
3153  
3154  
3155  
3156  
3157  
3158  
3159  
3160  
3161  
3162  
3163  
3164  
3165  
3166  
3167  
3168  
3169  
3170  
3171  
3172  
3173  
3174  
3175  
3176  
3177  
3178  
3179  
3180  
3181  
3182  
3183  
3184  
3185  
3186  
3187  
3188  
3189  
3190  
3191  
3192  
3193  
3194

(n) (U) The following USSTRATCOM Component commanders have specific tasks in support of CONPLAN 8039:

1 (U) Joint Functional Component Command Global Strike & Integration (JFCC GSI) when directed will:

a (U) With component support, will maintain common situational awareness for the headquarters and incorporating CO capabilities into integrated solutions for USSTRATCOM operations as a supported commander.

b (U) Through the Global Operations Center (GOC), USSTRATCOM Integration Operations Center (SIOC) and Joint Planning Working Group (JPWG), will integrate IO with all USSTRATCOM capabilities to assure the range of military operations is provided for DOD activities and operations.

c (~~S//Rel to USA, AUS, GBR~~) Develop operational-level plans to (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) COAs must include various types of (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

d (~~S//Rel to USA, AUS, GBR~~) Establish a (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) cyberspace.

e (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) operations planning and (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) to JTF GNO and other components in order to provide (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

2 (U) Joint Task Force - Global Network Operations (JTF-GNO) when directed will:

a (U) Develop cyber-related defense COAs in coordination with, JFCC NW, JIOWC and affected C/S/As as applicable that deter or defeat unauthorized activity targeted against the DOD GIG. Submit to HQ USSTRATCOM for approval.

**SECRET**

- 3195 b (U) As directed, conduct strategic, global cyber-related
- 3196 defense operations to defend DOD's use of cyberspace.
- 3197
- 3198 c (U) Coordinate development and planning of cyber-
- 3199 related defense measures with DOD and non-DOD
- 3200 organizations and agencies. This includes
- 3201 coordination with the DHS through the US CERT and
- 3202 the NCRCG during actual or potential cyber incidents.
- 3203 Submit to HQ USSTRATCOM for approval.
- 3204
- 3205 d (U) Provide coordination and technical assistance to
- 3206 C/S/As to minimize and deconflict operational
- 3207 impacts resulting from changes in INFOCON levels.
- 3208 This includes coordination with the DHS through the
- 3209 US CERT and the NCRCG during actual or potential
- 3210 cyber incidents that may impact U.S. cyberspace
- 3211 outside the DOD GIG.
- 3212
- 3213 e (U) Provide the consolidation of information from the
- 3214 service CERTs to all appropriate C/S/As.
- 3215
- 3216 f (U) Coordinate for enhanced information sharing with
- 3217 allies, coalition partners and the private sector, based
- 3218 on approved Delegation of Disclosure Authority Official
- 3219 memorandum (ref k) and approved MOAs/MOUs.
- 3220
- 3221 g (U//~~FOUO~~) Coordinate with the Law Enforcement
- 3222 Counterintelligence Center (LECIC) Defense Criminal
- 3223 Investigative Organizations (DCIOs) Liaison Officers for
- 3224 support of Service, federal, state and local law
- 3225 enforcement and counterintelligence agencies to
- 3226 counter, mitigate or halt threats to the DOD GIG.
- 3227
- 3228 h (U) Monitor and analyze (b)(1) Sec 1.7(e) intrusions
- 3229 and other cyber incidents of interest against the DOD's
- 3230 use of cyberspace and provide operational impact
- 3231 assessments to CDRUSSTRATCOM in coordination
- 3232 with service CERTs, DOD and service intelligence
- 3233 agencies.
- 3234
- 3235 i (U) Monitor C/S/As compliance with IAVAs and
- 3236 status of waivers and advise CDRUSSTRATCOM on
- 3237 matters pertaining to vulnerabilities of DOD cyber
- 3238 systems.
- 3239

**SECRET**

**SECRET**

- 3240  
3241  
3242  
3243  
3244  
3245  
3246  
3247  
3248  
3249  
3250  
3251  
3252  
3253  
3254  
3255  
3256  
3257  
3258  
3259  
3260  
3261  
3262  
3263  
3264  
3265  
3266  
3267  
3268  
3269  
3270  
3271  
3272  
3273  
3274  
3275  
3276  
3277  
3278  
3279  
3280  
3281  
3282  
3283  
3284  
3285
- j (U) Provide situational awareness (e.g., COP) regarding the defensive status of the DOD GIG to C/S/As. This includes coordination with the DHS through the US CERT and the NCRCG during actual or potential cyber incidents.
  - k (U) Provide tactical warning to C/S/As for defense of the DOD GIG.
  - l (U) Sustain access to GIG backbone services.
  - m (U) Monitor INFOCON levels and implemented actions of C/S/As.
  - n (U) Provide and track waivers to selected INFOCON actions that cause unacceptable operational mission impact to C/S/As.
  - o (U) Coordinate with appropriate organizations to institute additional protection and defense measures to include using INFOCON procedures.
  - p (U) Provide operational assessment of GIG network performance after attacks or intrusions have occurred to HQ USSTRATCOM, SECDEF, CJCS and the C/S/As, as required.
  - q (U) Work with C/S/As, as required to develop assessment of operational impact of attacks and intrusions against DOD cyber systems.
  - r (U) Direct and coordinate restoration efforts. This includes determining and directing global alternate routing efforts and prioritization of network assets during network outages, attacks, and contingencies.
  - s (U) In response to network events or activities, as determined by CDRUSSTRATCOM or CDR JTF-GNO, Service Chiefs, or Secretaries, shall instantaneously attach Service CERTs/CIRTs to CDR JTF-GNO, who will exercise TACON upon contact with the service CERTs/CIRTs until such time that the responses to the events or activities are declared complete by CDR JTF-GNO, at which time Service Secretaries will resume control on the CERTs/CIRTs.

**SECRET**

**SECRET**

- 3286 t (U) Recommend changes to daily operations network
- 3287 configurations as a result of lessons learned.
- 3288
- 3289 u (U) Gather, analyze and report cyber-related defense
- 3290 combat assessment to CDRUSSTRATCOM.
- 3291
- 3292 v (U) Coordinate and recommend changes to Global
- 3293 INFOCON posture levels to CDRUSSTRATCOM.
- 3294
- 3295 w (U) Identify strategic, global cyber-related defense
- 3296 intelligence requirements to USSTRATCOM in
- 3297 coordination with the geographic Combatant
- 3298 Commanders.
- 3299
- 3300 x (U) Determine and forward adversary's intent,
- 3301 capability, and information to CDRUSSTRATCOM and
- 3302 assess the risk of returning to a pre-hostility
- 3303 configuration.
- 3304
- 3305 y (U) After a cyber incident, coordinate return to daily
- 3306 operations network configurations and operations with
- 3307 C/S/As as soon as feasible.
- 3308
- 3309 z (~~S//Rel to USA, AUS, GBR~~) Provide situational
- 3310 awareness of (b)(1) Sec 1.4(a)
- 3311 (b)(1) Sec 1.4(a)
- 3312
- 3313
- 3314 aa (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)
- 3315 (b)(1) Sec 1.4(a) Information Condition (INFOCON)
- 3316 exceptions from C/S/As.
- 3317
- 3318 bb (U) Coordinate cyber defense measures with C/S/As
- 3319 prior to implementation.
- 3320
- 3321 cc (U) Direct GIG operations and defense. Identify and
- 3322 advocate new desired characteristics and capabilities.
- 3323 C/S/As are responsible for implementing a network
- 3324 security baseline through a defense in depth strategy
- 3325 for their respective mission-critical, mission-essential
- 3326 and mission-support networks.
- 3327
- 3328 dd (U) Issue DOD-wide INFOCON level changes, based on
- 3329 assessed threats. Maintain awareness of INFOCON
- 3330 levels across the GIG and associated INFOCON
- 3331 implementation.

**SECRET**

**SECRET**

3332  
3333  
3334  
3335  
3336  
3337  
3338  
3339  
3340  
3341  
3342  
3343  
3344  
3345  
3346  
3347  
3348  
3349  
3350  
3351  
3352  
3353  
3354  
3355  
3356  
3357  
3358  
3359  
3360  
3361  
3362  
3363  
3364  
3365  
3366  
3367  
3368  
3369  
3370  
3371  
3372  
3373  
3374  
3375  
3376  
3377

ee (U) Assess awareness of the operational impacts of changing INFOCON levels and recommended mitigation actions.

ff (U) Provide policy, direction and guidance to C/S/As regarding increased defense, network assurance operations and deterrence measures.

gg (~~S//Rel to USA, AUS, GBR~~) Develop and coordinate plans to implement (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

hh (U) Execute defensive operations and cyber defense IAW SROE (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

ii (~~FOUO~~) Accept Operational Control (OPCON) of service Network Operations Security Centers (NOSCs). Direct Liaison Authority (DIRLAUTH) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) is authorized.

ii (U) Submit cyberspace defense COAs to HQ USSTRATCOM to assure minimal impact to operation of the DOD GIG.

kk (~~S//Rel to USA, AUS, GBR~~) Submit military (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) to HQ USSTRATCOM.

ll (~~S//Rel to USA, AUS, GBR~~) Coordinate with C/S/As (b)(1) Sec 1.4(a)

mm (~~S//Rel to USA, AUS, GBR~~) Direct and coordinate the (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

nn (~~S//REL to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) Coordinate with other USSTRATCOM components in the development of courses of action and for the (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

3378  
3379  
3380  
3381  
3382  
3383  
3384  
3385  
3386  
3387  
3388  
3389  
3390  
3391  
3392  
3393  
3394  
3395  
3396  
3397  
3398  
3399  
3400  
3401  
3402  
3403  
3404  
3405  
3406  
3407  
3408  
3409  
3410  
3411  
3412  
3413  
3414  
3415  
3416  
3417  
3418  
3419  
3420  
3421  
3422  
3423

- oo (U) Support Combatant Commands efforts to plan, coordinate, and conduct cyberspace and NETOPS activities.
- 3 (U) Joint Functional Component Command – Network Warfare (JFCC NW) when directed will:
  - a (~~S//Rel to USA, AUS, GBR~~) Provide the supported Commander (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) COAs. Coordinate COAs with JFCC GSI to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Options/COAs must describe the (b)(1) Sec 1.4(a) Each option/COA will address the (b)(1) Sec 1.4(a) and (b)(1) Sec 1.4(a) in support of the overall operation.
  - b (~~S//Rel to USA, AUS, GBR~~) Support JTF-GNO by providing (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)
  - c (~~S//Rel to USA, AUS, GBR~~) Coordinate (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) assets to achieve supported Commander objectives across all phases of the operation.
  - d (~~S//Rel to USA, AUS, GBR~~) Direct (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) the DOD GIG.
  - e (~~S//Rel to USA, AUS, GBR~~) Direct (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) use of cyberspace.
  - f (U) Coordinate employment of cyber warfare capabilities with JTF-GNO, JIOWC and other JFCCs. When directed, assume operational control (OPCON) or tactical control (TACON) of forces designated in the establishing deployment order.

**SECRET**

3424  
3425  
3426  
3427  
3428  
3429  
3430  
3431  
3432  
3433  
3434  
3435  
3436  
3437  
3438  
3439  
3440  
3441  
3442  
3443  
3444  
3445  
3446  
3447  
3448  
3449  
3450  
3451  
3452  
3453  
3454  
3455  
3456  
3457  
3458  
3459  
3460  
3461  
3462  
3463  
3464  
3465  
3466  
3467  
3468  
3469

g (~~S//Rel to USA, AUS, GBR~~) Develop COA recommendations for (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) USSTRATCOM missions and maintaining situational awareness for CDRUSSTRATCOM.

h (U//~~FOUO~~) Serve as the focal point for DoD (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

(1) (U) Support JTF-GNO in their (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) to ensure operations are integrated and synchronized.

(2) (U) Coordinate intelligence gain/loss and technical assessments with the Intelligence Community for each network warfare course of action.

(3) (U) Coordinate and deconflict USSTRATCOM courses of action and as directed, the courses of action in support of other JFCs with the Intelligence Community.

i (U) Support Combatant Commands efforts to plan, coordinate, and conduct cyberspace activities.

4 (U) Joint Information Operations Warfare Command (JIOWC) when directed will:

a (U) Provide CDRUSSTRATCOM staff, JFCC NW, and JTF-GNO planners with IO and Strategic Communication expertise , as required, to conduct contingency and crisis action planning.

b (~~S//Rel to USA, AUS, GBR~~) Coordinate with JFCC NW, JFCC GSI, and JTF-GNO to ensure JIOWC's (b)(1) Sec 1.4(a)

c (~~S//Rel to USA, AUS, GBR~~) Establish and execute an (b)(1) Sec 1.4(a)



**SECRET**

3470  
3471  
3472  
3473  
3474  
3475  
3476  
3477  
3478  
3479  
3480  
3481  
3482  
3483  
3484  
3485  
3486  
3487  
3488  
3489  
3490  
3491  
3492  
3493  
3494  
3495  
3496  
3497  
3498  
3499  
3500  
3501  
3502  
3503  
3504  
3505  
3506  
3507  
3508  
3509  
3510  
3511  
3512  
3513  
3514

(b)(1) Sec 1.4(a) in coordination with appropriate C/S/As.

d (~~S//Rel to USA, AUS, GBR~~) Develop and (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

e (~~S//Rel to USA, AUS, GBR~~) Fully coordinate and synchronize (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

5 (U) Combatant Commands when directed will:

a (U) Conduct operations in and through cyberspace within their AORs, and coordinate with USSTRATCOM planners, as required

b (U) Review and update prioritization assessment of networks to identify those that are mission-critical, mission-essential, and mission-support networks, and share information with USSTRATCOM contributing to global situation awareness.

c (~~S//Rel to USA, AUS, GBR~~) Nominate appropriate (b)(1) Sec 1.4(a)

d (U) Share (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)  
facilitating global situation awareness and tailored planning/operations.

e (U) Employ measures to ensure friendly forces are in compliance with all counter-vulnerabilities requirements.

f (~~S//Rel to USA, AUS, GBR~~) In coordination with USSTRATCOM, (b)(1) Sec 1.4(a) in support of CONPLAN 8039, to include (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

g (U) Enforce IAVA compliance within their specific enterprise.

**SECRET**

**SECRET**

3515  
3516  
3517  
3518  
3519  
3520  
3521  
3522  
3523  
3524  
3525  
3526  
3527  
3528  
3529  
3530  
3531  
3532  
3533  
3534  
3535  
3536  
3537  
3538  
3539  
3540  
3541  
3542  
3543  
3544  
3545  
3546  
3547  
3548  
3549  
3550  
3551  
3552  
3553  
3554  
3555  
3556  
3557  
3558  
3559  
3560

- h (U) Share operational assessments and technical reports to the JTF-GNO when network attacks and intrusions are targeted against computers and other cyber systems within respective AOR, to maintain awareness and enhance potential response and deterrent options.
- i (~~S//Rel to USA, AUS, GBR~~) Provide recommendations for (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) to CDRUSSTRATCOM.
- i (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) within respective AORs and AOIs.
- k (U) Be prepared to support USSTRATCOM and LEAs in crisis, consequence management, and combat assessment within respective AORs.
- l (U) Assist CDRUSSTRATCOM with (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)
- m (U) Per ref c, Combatant Commanders will deconflict and synchronize their planning with CDRUSSTRATCOM.
- 6 (U) Agencies. Specific agencies will be identified in Annex A.

  - a (U) General Tasks:

    - (1) (U) Share (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) awareness and tailored planning/operations.
    - (2) (U) Coordinate with USSTRATCOM on matters pertaining to CO. Implement DOD-wide CO directions from CDRUSSTRATCOM for applicable networks.
    - (3) (FOUO) Maintain DIRLAUTH with other Service and Agency (b)(1) Sec 1.7(e)

**SECRET**

- 3561 (4) ~~(FOUO)~~ Direct and monitor compliance (including
- 3562 CTOs, IAVAs, and INFOCON) of agency networks
- 3563 with approved DOD policies and procedures that
- 3564 regulate operations in the DOD GIG (see Annex C
- 3565 Operations) and report as required to JTF GNO.
- 3566
- 3567 (5) ~~(FOUO)~~ Share near-real time global situational
- 3568 awareness of Agency networks and systems to JTF-
- 3569 GNO. Provide a single POC/office to interface with
- 3570 JTF-GNO for this purpose.
- 3571
- 3572 (6) ~~(FOUO)~~ Coordinate, execute and/or direct
- 3573 troubleshooting and restoral actions for Agency
- 3574 networks and systems.
- 3575
- 3576 (7) ~~(FOUO)~~ Monitor Named Areas of Interest (NAIs) as
- 3577 tasked by JTF-GNO to detect threat activity against
- 3578 the DOD GIG (see Annex C).
- 3579
- 3580 (8) ~~(FOUO)~~ Implement response actions as directed by
- 3581 JTF-GNO (IAW SROE), to correct faults, defeat
- 3582 threat activity, and deliver priority information
- 3583 across the DOD GIG (see Annex C).
- 3584
- 3585 (9) ~~(FOUO)~~ Implement contingency operations as
- 3586 directed by JTF-GNO to restore capability and
- 3587 strengthen the DOD GIG against further faults,
- 3588 threats and information gaps across the DOD GIG
- 3589 (see Annex C).
- 3590
- 3591 (10) ~~(FOUO)~~ Report to JTF-GNO status of (b)(1) Sec 1.7(e)
- 3592 (b)(1) Sec 1.7(e)
- 3593
- 3594
- 3595
- 3596 (11) ~~(FOUO)~~ Establish, in coordination with JTF-
- 3597 GNO, procedures for dissemination of NETOPS
- 3598 related advisories, alerts, and warning notices.
- 3599
- 3600 (12) ~~(FOUO)~~ Conduct nodal analysis of agency
- 3601 networks to determine Critical Nodes and provide
- 3602 Critical Node list to JTF-GNO.
- 3603
- 3604 (13) ~~(FOUO)~~ Share defense plans of critical nodes
- 3605 against physical and virtual threats with JTF-GNO

**SECRET**

**SECRET**

3606  
3607  
3608  
3609  
3610  
3611  
3612  
3613  
3614  
3615  
3616  
3617  
3618  
3619  
3620  
3621  
3622  
3623  
3624  
3625  
3626  
3627  
3628  
3629  
3630  
3631  
3632  
3633  
3634  
3635  
3636  
3637  
3638  
3639  
3640  
3641  
3642  
3643  
3644  
3645  
3646  
3647  
3648  
3649  
3650

facilitating global situation awareness and tailored planning/operations.

**b (U) Specific Organizations.**

**(1) (U)** (b)(1) Sec 1.7(e)

a. **(U//FOUO)** Provide to C/S/As (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

actions, as well as mitigation strategies.

b. **(S//Rel to USA, USA, AUS)** Develop, in cooperation with USSTRATCOM and its Components, (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

Provide to C/S/As (b)(1) Sec 1.4(a)  
defense related tools and their associated training and documentation.

c. **(S//Rel to USA, AUS, GBR)** (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) and related techniques.

d. **(U//FOUO)** (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

advice.

e. **(S//Rel to USA, AUS, GBR)** (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

f. **(S//Rel to USA, AUS, GBR)** Provide to C/S/As consolidated (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

**SECRET**

3651  
3652  
3653  
3654  
3655  
3656  
3657  
3658  
3659  
3660  
3661  
3662  
3663  
3664  
3665  
3666  
3667  
3668  
3669  
3670  
3671  
3672  
3673  
3674  
3675  
3676  
3677  
3678  
3679  
3680  
3681  
3682  
3683  
3684  
3685  
3686  
3687  
3688  
3689  
3690  
3691  
3692  
3693  
3694  
3695  
3696

g. (U//FOUO) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

h. (~~S//Rel to USA, AUS, GBR~~) Coordinate with  
(b)(1) Sec 1.4(a)

i. (U//FOUO) Provide to C/S/As (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

j. U//FOUO Provide to C/S/As (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)  
(U//FOUO) Provide to C/S/As (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

k. (U//FOUO) Share with C/S/As (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

l. (U//FOUO) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

(2) (U) (b)(1) Sec 1.7(e)

a. (U) Provide CDRUSSTRATCOM with the  
(b)(1) Sec 1.7(e)

b. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

**SECRET**

**SECRET**

3697  
3698  
3699  
3700  
3701  
3702  
3703  
3704  
3705  
3706  
3707  
3708  
3709  
3710  
3711  
3712  
3713  
3714  
3715  
3716  
3717  
3718  
3719  
3720  
3721  
3722  
3723  
3724  
3725  
3726  
3727  
3728  
3729  
3730  
3731  
3732  
3733  
3734  
3735  
3736  
3737  
3738  
3739  
3740  
3741  
3742

(b)(1) Sec 1.7(e)

c. (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

d. (S//Rel to USA, AUS, GBR) Coordinate with  
(b)(1) Sec 1.4(a)

e. (S//Rel to USA, AUS, GBR) When required to  
(b)(1) Sec 1.4(a)

f. (U) Assist CDRUSSTRATCOM (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

g. (U) Recommend, manage and perform (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

h. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

USSTRATCOM.

i. (U) Coordinate with JTF-GNO in the  
(b)(1) Sec 1.7(e)

j. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

**SECRET**

3743  
3744  
3745  
3746  
3747  
3748  
3749  
3750  
3751  
3752  
3753  
3754  
3755  
3756  
3757  
3758  
3759  
3760  
3761  
3762  
3763  
3764  
3765  
3766  
3767  
3768  
3769  
3770  
3771  
3772  
3773  
3774  
3775  
3776  
3777  
3778  
3779  
3780  
3781  
3782  
3783  
3784  
3785  
3786  
3787  
3788

k. (U) Coordinate with C/S/As, (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

l. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

m. (U) In coordination with JTF-GNO, (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

n. (U) Assist JTF-GNO in (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

o. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

p. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) to ensure interoperability with the  
DOD GIG.

(3) (U) (b)(1) Sec 1.7(e)

a. (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
CONPLAN 8039. The scope of (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

b. (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

**SECRET**

3789  
3790  
3791  
3792  
3793  
3794  
3795  
3796  
3797  
3798  
3799  
3800  
3801  
3802  
3803  
3804  
3805  
3806  
3807  
3808  
3809  
3810  
3811  
3812  
3813  
3814  
3815  
3816  
3817  
3818  
3819  
3820  
3821  
3822  
3823  
3824  
3825  
3826  
3827  
3828  
3829  
3830  
3831  
3832  
3833  
3834

c. (~~S//Rel to USA, AUS, GBR~~) Coordinate with

(b)(1) Sec 1.4(a)

(4) (U) (b)(1) Sec 1.7(e)

a. (~~S//Rel to USA, AUS, GBR~~) Identify internal

(b)(1) Sec 1.4(a)

b. (~~S//Rel to USA, AUS, GBR~~) Provide

USSTRATCOM (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

d. (U) Coordinating Instructions.

(1) (~~S//Rel to USA, AUS, GBR~~) Conditions for execution.

CONPLAN 8039 is effective for planning purposes upon receipt. When CDRUSSTRATCOM or SECDEF approves this plan, it will

(b)(1) Sec 1.4(a)

(2) (U) Direct liaison is authorized among CDRUSSTRATCOM components, C/S/As, supporting commands and planning headquarters. When developing supporting plans, maintain liaison with CDRUSSTRATCOM.

(3) (U) Component commands will develop supporting plans to CONPLAN 8039 and submit them to USSTRATCOM when tasked by CDRUSSTRATCOM.

(4) (U) ROE will be IAW ref o and modified with supplemental ROE as appropriate.

(5) (U) All CO forces supporting the CDRUSSTRATCOM mission will immediately establish liaison with CDRUSSTRATCOM LNO upon arriving in theater.



**SECRET**

3835  
3836  
3837  
3838  
3839  
3840  
3841  
3842  
3843  
3844  
3845  
3846  
3847  
3848  
3849  
3850  
3851  
3852  
3853  
3854  
3855  
3856  
3857  
3858  
3859  
3860  
3861  
3862  
3863  
3864  
3865  
3866  
3867  
3868  
3869  
3870  
3871  
3872  
3873  
3874  
3875  
3876  
3877  
3878

(6) (U) Commander's Critical Information Requirements (CCIR).  
The following are examples of CCIRs:

(a) (U) (b)(1) Sec 1.7(e) (See Annex B)

(b) (U) Friendly Forces Information Requirements (FFIRs). The following constitute FFIRs:

1 (U) Any increase/decrease in INFOCON worldwide.

2 (U) Any event (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

3 (U) Any event that (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

a (U) Any (b)(1) Sec 1.7(e) DOD  
GIG.

b (U) Any (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

c (U) Any access to the DOD GIG by unauthorized persons obtaining privileged user, administrator or root level access.

d (U) Any (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

e (U) Any (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

f (U) Any (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)  
imminently conduct these operations.

g (U) Any (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

**SECRET**

3879  
3880  
3881  
3882  
3883  
3884  
3885  
3886  
3887  
3888  
3889  
3890  
3891  
3892  
3893  
3894  
3895  
3896  
3897  
3898  
3899  
3900  
3901  
3902  
3903  
3904  
3905  
3906  
3907  
3908  
3909  
3910  
3911  
3912  
3913  
3914  
3915  
3916  
3917  
3918  
3919  
3920  
3921  
3922  
3923  
3924

h (U) Any (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)  
operational networks.

i (U) Any (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

i (U) Any (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

k (U) Any (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)  
C/S/As (e.g., GCSS, GCCS and DMS).

l (U) Any root level access, on a system shared by the DOD GIG, using new methods that exploit a system's vulnerabilities.

m (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) C/S/As (e.g., GCSS, GCCS and DMS).

4 (U) Any event that negatively affects execution of the Information Operations mission.

(c) (U) Essential Elements of Information (EEI).

1 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

2 (S//Rel to USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

3 (C) (b)(1) Sec 1.4(a) DOD GIG.

4 (~~S//Rel to USA, AUS, GBR~~) the DOD GIG (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

5 (C) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

**SECRET**

3925  
3926  
3927  
3928  
3929  
3930  
3931  
3932  
3933  
3934  
3935  
3936  
3937  
3938  
3939  
3940  
3941  
3942  
3943  
3944  
3945  
3946  
3947  
3948  
3949  
3950  
3951  
3952  
3953  
3954  
3955  
3956  
3957  
3958  
3959  
3960  
3961  
3962  
3963  
3964  
3965  
3966  
3967  
3968  
3969

6 (~~S//Rel to USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
DOD GIG and C4I systems.

- 4. (U) Administration and Logistics.
  - a. (U) Concept of Support. Supply support will be IAW Service doctrine. Teams consisting of tailored HQ USSTRATCOM, JFCC NW, JTF-GNO, JIOWC and Service component personnel will be provided administrative and logistical support by the requesting command.
  - b. (U) Logistics. CONPLAN 8039 is logistically supportable. Cyberspace forces may need to deploy under an ad hoc TPFDL.
  - c. (U) Personnel.
    - (1) (U) The parent command or agency will retain administrative responsibility for USSTRATCOM augmentation forces.
    - (2) (U) The appropriate USSTRATCOM Service component will assume administrative responsibility for military personnel (Active, Reserve or National Guard) assigned to USSTRATCOM's subordinate units.
    - (3) (U) Personnel accountability and direct management of military and DOD civilian resources (i.e., casualties, replacements, additional forces, etc.) will be the responsibility of the service component or the parent command or agency.
  - d. (U) Public Affairs (PA). The supported Combatant Command for CO in the operation will handle PA. When CDRUSSTRATCOM is the supported commander, the USSTRATCOM public affairs office will handle PA.
  - e. (U) Civil Affairs. Civil Affairs planning will be provided by U.S. Army Reserve Civil Affairs forces assigned to USSTRATCOM. CDRUSSTRATCOM will plan and execute Civil Affairs supporting CO when acting as the supported commander. Regional commanders will execute their Civil Affairs support to CO with organic personnel, JIOWC Combatant Commander teams as required, and U.S. Army Reserve Civil Affairs forces, as required.
  - f. (U) Meteorological and Oceanographic (METOC) Services. METOC in support of CO will be provided by USSTRATCOM JFCC GSI METOC Branch (JFCC GSI J332.)

**SECRET**

- 3970 g. (U) Geospatial Information and Services. Geospatial information  
3971 in support of CO will be provided by USSTRATCOM/J2, in  
3972 coordination with NGA.  
3973
- 3974 h. (U) Medical Services. The Combatant Commander where CO is  
3975 being conducted will provide medical services for supporting  
3976 personnel.  
3977
- 3978 5. (U) Command and Control (C2). The Service CO C2 structure as it  
3979 applies to USSTRATCOM, JFCC NW, and JTF-GNO is not a standardized  
3980 component structure, as the Army, Air Force, Navy and Marine Corps  
3981 each have organized their cyberspace activities differently. See Annex J  
3982 for specific C2 relationships.  
3983
- 3984
- 3985 Kevin P. Chilton  
3986 General, USAF  
3987 Commander  
3988
- 3989
- 3990
- 3991 Annexes:  
3992
- 3993 A--Task Organization  
3994 B--Intelligence  
3995 C--Operations  
3996 F--Public Affairs  
3997 J--Command Relationships  
3998 K--Command, Control, Communications and Computer Systems  
3999 N--Space Operations  
4000 S--Special Technical Operations  
4001 V--Interagency  
4002 Y--Strategic Communication  
4003 Z--Distribution  
4004  
4005  
4006

**SECRET**

DANIEL L. KARBLER  
Major General, U.S. Army  
Chief of Staff  
U.S. Strategic Command

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AFB NE 68113-6500  
28 February 2008

2 ANNEX A TO USSTRATCOM CONPLAN 8039 (U)

3 (U) OPR: JFCC NW J52

4 TASK ORGANIZATION (U)

5  
6 (U) References: Refer to Base Plan.

7  
8 1. (U) Task Organization

9 a. (U) Supporting or Assigned Forces. While many DOD Components do  
10 not have organizations dedicated solely to cyber operations, there are DOD  
11 organizations not assigned to USSTRATCOM that have cyber capabilities. This  
12 annex identifies supporting or subordinate organizations capable of conducting  
13 or providing support to the cyber operations mission. To provide the broadest  
14 range of military capability, these forces will be made available to  
15 USSTRATCOM through various command relationships (Refer to Annex J,  
16 Command Relationships). Table 1 lists organizations that are designated in  
17 support of USSTRATCOM for CONPLAN 8039. Table 2 lists organizations  
18 subordinate or assigned to USSTRATCOM for CONPLAN 8039.

19 b. (U) (b)(1) Sec 1.7(e) The majority of these  
20 forces (b)(1) Sec 1.7(e) accomplish assigned tasks.  
21 For this reason, a (b)(1) Sec 1.7(e) is not included in this annex. (b)(1) Sec 1.7(e)  
22 required, it will be developed for a (b)(1) Sec 1.7(e)

23 (b)(1) Sec 1.7(e)

24 c. (U) Shortfall Identification. (b)(1) Sec 1.7(e)

25 (b)(1) Sec 1.7(e)

26  
27 (b)(1) Sec 1.7(e) It will also identify the forces  
28 shortfall (if required) that normally accompanies Annex A, Task Organization.

29 d. (U) Organizational Relationships. Responsibilities and organizational  
30 relationships are discussed in Annex J, Command Relationships.

31 2. (U) Supporting Organizations. The following commands or organizations are  
32 identified to provide support to USSTRATCOM for CONPLAN 8039.

33  
**SECRET**

# SECRET

ORGANIZATION	COMMANDER
US European Command	CDRUSEUCOM
US Pacific Command	CDRUSPACOM
US Joint Forces Command	CDRUSJFCOM
US Transportation Command	CDRUSTRANSCOM
US Central Command	CDRUSCENTCOM
US Special Operations Command	CDRUSSOCOM
US Northern Command	CDRUSNORTHCOM
US Southern Command	CDRUSSOUTHCOM
US Africa Command	CDRUSAFRICOM
US Element North American Aerospace Command	CDRUSELEMNORAD
US Navy	CNO
US Air Force	CSAF
US Army	CSA
US Marine Corps	CMC
Marine Corps Intelligence Activity	CO MCIA
Air Combat Command	COMACC
Central Intelligence Agency	DCIA
<u>Defense Advanced Research Projects Agency</u>	<u>DARPA</u>
<u>Defense Business Transformation Agency</u>	<u>BTA</u>
<u>Defense Legal Services Agency</u>	<u>DLSA</u>
<u>Defense Commissary Agency</u>	<u>DeCA</u>
<u>Defense Contract Audit Agency</u>	<u>DCAA</u>
<u>Defense Contract Management Agency</u>	<u>DIRDCMA</u>
<u>Defense Finance and Accounting Service</u>	<u>DFAS</u>
<u>Defense Information Systems Agency</u>	<u>DIRDISA</u>
<u>Defense Intelligence Agency</u>	<u>DIRDIA</u>
<u>Defense Logistics Agency</u>	<u>DIRDLA</u>
<u>Defense Security Cooperation Agency</u>	<u>DSCA</u>
<u>Defense Security Service</u>	<u>DSS</u>
<u>Defense Threat Reduction Agency</u>	<u>DIRDTRA</u>
<u>Missile Defense Agency</u>	<u>MDA</u>
<u>National Geospatial-Intelligence Agency</u>	<u>NGA</u>
<u>National Security Agency/Central Security Service</u>	<u>DIRNSA</u>
<u>Pentagon Force Protection Agency</u>	<u>PFPA</u>
<u>American Forces Information Service</u>	<u>AFIS</u>
<u>Defense POW/MP Office</u>	<u>DPMO</u>
<u>Defense Technology Security Administration</u>	<u>DTSA</u>
<u>Defense Technical Information Center</u>	<u>DTIC</u>
<u>DOD Counterintelligence Field Activity</u>	<u>CIFA</u>
<u>DOD Education Activity</u>	<u>DoDEA</u>
<u>DOD Human Resources Activity</u>	<u>DoDHRA</u>
<u>DOD Test Resource Management Center</u>	<u>TRMC</u>

SECRET

**SECRET**

<u>Office of Economic Adjustment</u>	<u>OEA</u>
<u>TRICARE Management Activity</u>	<u>TMA</u>
<u>Washington Headquarters Services</u>	<u>WHS</u>
<u>USAF Intelligence, Surveillance and Reconnaissance Agency</u>	<u>CDR AFISRA</u>
<u>USA Intelligence and Security Command</u>	<u>CDR INSCOM</u>
<u>USN Naval Security Group</u>	<u>COMNAVSECGRU</u>
<u>National Guard Bureau</u>	<u>CHIEF, NGB</u>
<u>Air Force Office of Special Investigations</u>	<u>AFOSI</u>
<u>Naval Criminal Investigative Service</u>	<u>NCIS</u>
<u>USA Criminal Investigation Division</u>	<u>CDR CID</u>
<u>Strategic Systems Programs/Naval Surface Warfare Center</u>	<u>SSP/NSWCDD</u>
<u>Joint Warfare Analysis Center</u>	<u>CDR, JWAC</u>
Table 1: Supporting Organizations (U)	

34

35

Table 1: Supporting Organizations (U)

36

37

3. (U) Subordinate Commands. The following commands are designated as subordinate commands for CONPLAN 8039.

SUBORDINATE COMMANDS	COMMANDER
JFCC Global Strike and Integration	CDR JFCC GSI
JFCC Intelligence, Surveillance, and Reconnaissance	CDR JFCC ISR
JFCC Integrated Missile Defense	CDR JFCC IMD
JFCC Network Warfare	CDR JFCC NW
JTF _ Global Network Operations	CDR JTF GNO
JFCC Space	CDR JFCC SPACE
STRATCOM Center for Combating WMD	CDR SCC WMD
Joint Information Operations Warfare Command	CDR JIOWC
Air Force Strategic Global Strike	AFSTRAT-GS/CC
Air Force Strategic Space	AFSTRAT-SPACE/CC
Marine Forces USSTRATCOM	COMMARFORSTRAT
US Fleet Forces Command	COMFLTFORCOM
Space and Missile Defense Command/Army Strategic Forces	CDR SMDC/ARSTRAT

38

39

Table 2: Subordinate Organizations (U)

**SECRET**

40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63

Kevin P. Chilton  
General, USAF  
Commander

Appendixes:

1--(U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

2--(U) Shortfall Identification (Maintained in (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

3--(U) Military Deterrent Options (S)

Mark H. Owen  
Brigadier General, USAF  
Director, Plans and Policy



**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE NE 68113-6500  
28 February 2008

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30

APPENDIX 3 TO ANNEX A TO USSTRATCOM CONPLAN 8039(U)

(U) OPR: JFCC NW J52

(b)(1) Sec 1.7(e) (U)

(U) References: Refer to Base Plan.

1. (U) Situation. The USG harnesses all aspects of national power through the application of diplomatic, informational, economic and military deterrent options. This annex discusses (b)(1) Sec 1.7(e) to facilitate the objectives of CONPLAN 8039, Cyberspace Operation. (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) available to CDRUSSTRATCOM are implemented in the planning process. CDRUSSTRATCOM working with the affected Geographical Combatant Commander (GCC) will recommend (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) present a menu of choices for recommendation to the (b)(1) Sec 1.7(e). Should deterrence fail, (b)(1) Sec 1.7(e) freedom of action in cyberspace.

a. (U) Friendly. Refer to Base Plan and Annex A (Task Organization).

b. (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

c. (U) Assumptions. Refer to Base Plan.

d. (U) Legal Considerations. Refer to Base plan and Appendix 8 (Rules of Engagement) to Annex C (Operations).

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (e), and (g)~~  
~~Declassify on: 06 December 2032~~

SECRET

31 a. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
32 (b)(1) Sec 1.4(a)  
33  
34  
35 (b)(1) Sec 1.4(a) potential threats to US interests.

36 b. (S//REL USA, AUS, GBR) Elements of National Power. An effective  
37 (b)(1) Sec 1.4(a)  
38  
39  
40 (b)(1) Sec 1.4(a) from the  
41 following categories may be implemented individually or in packages as  
42 appropriate to best meet the particular situation.

43 (1) (U) (b)(1) Sec 1.7(e)  
44 (b)(1) Sec 1.7(e) They may pursue measures to increase (b)(1) Sec 1.7(e)  
45 (b)(1) Sec 1.7(e) Other actions include measures to (b)(1) Sec 1.7(e)  
46 (b)(1) Sec 1.7(e) options may also seek to gain support from the  
47 (b)(1) Sec 1.7(e)

48 (2) (U) (b)(1) Sec 1.7(e)  
49 (b)(1) Sec 1.7(e)  
50  
51 (b)(1) Sec 1.7(e) to maintain freedom of action in cyberspace. These options may be  
52 (b)(1) Sec 1.7(e)

53 (3) (U) (b)(1) Sec 1.7(e) increase/highlight assistance  
54 already provided (b)(1) Sec 1.7(e)

55 4. (U) Administration and Logistics. – Not used.

56 5. (U) Command and Control. – Refer to Base Plan and Annex J (Command  
57 Relationships).

58

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AFB NE 68113-6500  
26 February 2008

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39

ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)  
(U) OPR: HQ USSTRATCOM/J23 INTELLIGENCE (U)  
28 February 2008  
(U) References:

a. (U) Joint Publication 2-0, Joint Doctrine for Intelligence Support to Operations, 9 March 2000 (U).

b. (U) Draft CJCSM 3314.01, Chairman of the Joint Chiefs of Staff Manual, Intelligence Campaign Planning Guidance, 30 November 2007 (U).

c. (U) (b)(1) Sec 1.7(e) updated semi-annually, (S//SI//NF).

d. (U) Joint Publication 2-01.3, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace, 24 May 2000 (U).

e. (U) National Intelligence Support Plan (NISP) in Support of USSTRATCOM CONPLAN 8039, Date TBD (S//COMINT//REL).

f. (U//FOUO) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (S//SI).

g. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (TS//SI).

h. (U) (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) (TS//SI).

i. (U//~~FOUO~~) CJCSI 3110.02D, Intelligence Planning Objectives, Guidance and Tasks, 5 March 2003 (S).

j. (U//~~FOUO~~) DCID 7/3, Information Operations and Intelligence Community Related Activities, 1 July 1999.

1. (U) 1. (U) Situation. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) It is designed to provide intelligence

Classified by: Multiple Sources  
Reason: 1.4(a), (e), and (g)  
Declassify on: 26 February 2032

**SECRET**

**SECRET**

40 information at the strategic level that may be applicable to any state or non-  
41 state actor with a cyberspace capability and access or intent to use cyberspace  
42 to threaten U.S. networks. (b)(1) Sec 1.7(e)

43 (b)(1) Sec 1.7(e)

44  
45 a. (~~S//REL USA, AUS, GBR~~) Characteristics of the Area. The cyberspace  
46 environment is global in scale and is characterized by the use of electronics to  
47 store, modify, and exchange data via networked systems and associated  
48 physical infrastructures. The potential operational area is the entire  
49 cyberspace domain. [See the CONPLAN 8039 Base Plan paragraph 1 for a  
50 detailed description of Characteristics of Area / Area of Concern, Area of  
51 Interest (AOI), Area of Responsibility (AOR), Operational Area (AO), and Centers  
52 of Gravity (COGs).] The primary focus is to defend the DoD Global Information  
53 Grid (GIG) and (b)(1) Sec 1.4(a)

54 (b)(1) Sec 1.4(a)

58  
59 b. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

60 (b)(1) Sec 1.4(a)

73  
74 (1) (U) End State and Courses of Action

75  
76 (a) (~~S//REL USA, AUS, GBR~~) The foundations of intent (b)(1) Sec 1.4(a)

77 (b)(1) Sec 1.4(a)

78  
79  
80 Also included in this plan are (b)(1) Sec 1.4(a)

81 (b)(1) Sec 1.4(a)

82 (b)(1) Sec 1.4(a)

83 states such as:

end

**SECRET**

85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130

1. (S//REL USA, AUS, GBR USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2. (S//REL USA, AUS, GBR USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

3. (S//REL USA, AUS, GBR USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b) (C//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) full scope  
cyberspace operations capabilities (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

**SECRET**

131 (b)(1) Sec 1.4(a) including  
132 (b)(1) Sec 1.4(a)  
133 cyberspace programs. (b)(1) Sec 1.4(a)  
134 (b)(1) Sec 1.4(a) residing or transiting DoD information systems.  
135

136 (c) (U//~~FOUO~~) (b)(1) Sec 1.7(e) to include  
137 hackers, terrorists, insiders, and criminals, intend to access, deny, degrade, exploit, or modify  
138 data residing on U.S. cyberspace systems. (b)(1) Sec 1.7(e)

139 (b)(1) Sec 1.7(e)  
140  
141  
142  
143  
144  
145  
146

147  
148 (2) (U) (b)(1) Sec 1.7(e)  
149 (b)(1) Sec 1.7(e)  
150

151 (3) (~~C//REL USA, AUS, GBR~~) Capability to Collect, Process, and  
152 Disseminate Intelligence. (b)(1) Sec 1.4(a)  
153 (b)(1) Sec 1.4(a)  
154  
155  
156

157  
158 c. (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Friendly. Cyberspace  
159 operations require a (b)(1) Sec 1.4(a)  
160 effort. See the NISP to this CONPLAN for additional details on friendly  
161 intelligence capabilities and activities.  
162

163 (1) (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) DoD intelligence  
164 organizations (b)(1) Sec 1.4(a)  
165 (b)(1) Sec 1.4(a) conduct intelligence operations  
166 in support of cyberspace operations. DoD Intelligence must also develop or  
167 improve the capability to:  
168

169 (a) (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Provide (b)(1) Sec 1.4(a)  
170 (b)(1) Sec 1.4(a)  
171

172  
173 (b) (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Improve DOD's  
174 understanding of cyberspace networks. (b)(1) Sec 1.4(a)  
175 (b)(1) Sec 1.4(a)  
176

177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) See CONPLAN 8039 Base Plan for more details concerning (b)(1) Sec 1.4(a)

(c) (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Apportion intelligence assets (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(d) (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Prioritize efforts as directed by combatant command Joint Intelligence Operations Centers (JIOCs) and as illustrated by the CONPLAN 8039 (b)(1) Sec 1.4(a)

(2) (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Combatant command J2s will assess the effectiveness of the CONPLAN 8039 IP effort, including the (b)(1) Sec 1.4(a) this annex, the NISP, associated Functional Support Plans (FSPs), and other supporting documentation and processes in their respective AORs and forward (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) Forward ISR-related shortfalls for cyberspace operations to USSTRATCOM/J8 for advocacy and support.

d. (U) Legal Considerations. Given the unique nature of cyberspace, the legal framework associated with intelligence collection in support of cyberspace operations must be well understood. (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) All intelligence operations under this plan will be conducted in compliance with applicable U.S. domestic and international law. In particular, intelligence activities (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) Additional legal considerations can be found in the CONPLAN 8039 Base Plan.

2. (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Mission. Commander, US Strategic Command, plans and directs integrated DoD cyber operations to (b)(1) Sec 1.4(a)

interests. See NISP Base Plan for the National Intelligence Mission Statement

**SECRET**

223 3. (U) Execution

224  
225 a. (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Concept of Intelligence  
226 Operations. This annex is the base document for the cyberspace operations IP  
227 effort. It outlines the intelligence community support for USSTRATCOM's  
228 CONPLAN 8039 Cyberspace Operations and the Military Strategic Framework  
229 identified in the National Military Strategy for Cyberspace Operations. The goal

230 (b)(1) Sec 1.4(a)  
231  
232  
233  
234

235 (1) (~~S//REL USA, AUS, GBR USA, AUS, GBR~~) Purpose and Means. See  
236 CONPLAN 8039 Base Plan for the overall purpose. The 2005 Contingency  
237 Planning Guidance (CPG) advises the Chairman, Joint Chiefs of Staff (CJCS), to

238 (b)(1) Sec 1.4(a)  
239  
240  
241  
242  
243  
244

245 This annex provides guidance and direction to the (b)(1) Sec 1.4(a) that supports  
246 USSTRATCOM CONPLAN 8039 planning and execution, and combatant  
247 command cyberspace operations planning. (b)(1) Sec 1.4(a)

248 (b)(1) Sec 1.4(a)  
249

250 support cyberspace operations. Specifically, the CONPLAN 8039 (b)(1) Sec 1.4(a)

251  
252 (a) (U) Develop intelligence requirements and tasks and establish a  
253 common framework to understand the threat posed by state and non-state  
254 actors that have the capability and intent to threaten U.S. cyberspace.

255  
256 (b) (U) Designate missions, roles, and responsibilities for DoD  
257 intelligence agencies in support of combatant command execution of  
258 cyberspace operations planning and operations.

259  
260 (c) (U) Integrate and synchronize with intelligence plans of (b)(1) Sec 1.7(e)

261 (b)(1) Sec 1.7(e)  
262

263 (d) (U) Describe an integrated operational architecture to facilitate the  
264 development and dissemination of an intelligence (b)(1) Sec 1.7(e)

265 (b)(1) Sec 1.7(e)  
266

267 (e) (U) Identify doctrine, organization, training, material, leadership  
268 and education, and personnel shortfalls to successfully conduct cyberspace



SECRET

269 intelligence operations and develop mitigation strategies and responsibilities to  
270 correct them.

271  
272 (f) (U) Identify intelligence collection, analysis, and production  
273 requirements, thereby allowing (b)(1) Sec 1.7(e)  
274 (b)(1) Sec 1.7(e) responsibilities and allowing  
275 USSTRATCOM to advocate for solutions to shortfalls.

276  
277 (g) (U) Improve intelligence collection, analysis, and production  
278 capabilities (b)(1) Sec 1.7(e)  
279 (b)(1) Sec 1.7(e) cyberspace activities.

281 (2) (~~S//REL USA, AUS, GBR~~) General. CONPLAN 8039 follows an effects-  
282 based planning construct and is organized along the (b)(1) Sec 1.4(a)

283 (b)(1) Sec 1.4(a)  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295

296 (3) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Responsibilities.  
297 USSTRATCOM is charged with leading the (b)(1) Sec 1.4(a) for cyberspace operations

298 (b)(1) Sec 1.4(a)  
299  
300  
301  
302

303 (b)(1) Sec 1.4(a) See the NISP for additional details on the  
304 CONPLAN 8039 (b)(1) Sec 1.4(a)  
305 (b)(1) Sec 1.4(a)

306  
307 (4) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

308 (b)(1) Sec 1.4(a)  
309  
310  
311  
312  
313  
314

SECRET

315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360

(b)(1) Sec 1.4(a)

(a) (~~S//REL USA, AUS, GBR~~) Identify and understand (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) A clear understanding of these concepts is required to conduct an effective cyberspace operations campaign. Intelligence support is required for friendly forces to (b)(1) Sec 1.4(a) that allow the U.S. to

(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) cyberspace activity  
(b)(1) Sec 1.4(a)

(c) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) cyberspace related activity. (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(5) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(6) (U) National Intelligence Support

(a) (~~S//REL USA, AUS, GBR~~) Per (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) directed plan. Combatant commands (b)(1) Sec 1.4(a) will provide rationale to (b)(1) Sec 1.4(a)

(b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406

(b)(1) Sec 1.4(a)

(c) (~~S//REL USA, AUS, GBR~~) The NISP, (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(d) (U) USSTRATCOM JFCC-ISR provides the ISR Support Plan (ISRSP), which is also part of the NISP. The ISRSP will outline ISR capabilities and requirements to be performed both day-to-day and during crisis.

(7) (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

b. (U) Tasks

(1) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) cyberspace operations requirements.

(2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) and  
(b)(1) Sec 1.4(a) for conducting cyberspace intelligence operations.

(3) (U) Develop strategic cyberspace operations (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) Essential Elements of Information (EEIs), (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

(4) (U) In conjunction with USD(I) and (b)(1) Sec 1.7(e) develop Memorandum of Agreement/Command Arrangement Agreements where necessary.

(5) (U) Conduct required cyberspace operations IPRs.

**SECRET**

407 (6) (U) Monitor cyberspace I&W indicators.

408  
409 (7) (U) Establish strategic priorities for cyber threats (b)(1) Sec 1.7(e)

410 (b)(1) Sec 1.7(e)

411  
412 (8) (U) Support combatant command (b)(1) Sec 1.7(e) cyberspace operations  
413 requirements.

414  
415 (9) (U) Monitor day-to-day execution of the CONPLAN 8039 (b)(1) Sec 1.7(e) and  
416 identify or report changes in the ability of DoD Intelligence to provide the  
417 support identified in the ITL to USSTRATCOM.

418  
419 (10) (U) Assess DoD cyberspace intelligence capabilities and determine if

420 (b)(1) Sec 1.7(e)

421  
422 (11) (~~S//REL USA, AUS, GBR~~) Integrate CONPLAN 8039 (b)(1) Sec 1.4(a) with other  
423 USSTRATCOM global plans.

424  
425 (12) (U) Participate, as required, in national-level cyberspace operations  
426 intelligence planning and coordination efforts.

427  
428 c. (U) Procedures for processing (b)(1) Sec 1.7(e) is  
429 combatant command dependent and will be promulgated in the various  
430 combatant command CONPLANS and OPLANS. At USSTRATCOM, the J2 is  
431 responsible for processing (b)(1) Sec 1.7(e)

432  
433 d. (U) (b)(1) Sec 1.7(e)

434 (b)(1) Sec 1.7(e)

435  
436 e. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
437 agencies contributing to this (b)(1) Sec 1.4(a) effort have been identified in the CONPLAN

438 (b)(1) Sec 1.4(a)

440  
441  
442  
443  
444  
445  
446 support of CONPLAN 8039 requirements. See the NISP for detailed information  
447 on (b)(1) Sec 1.4(a)

448  
449 (1) (U) (b)(1) Sec 1.7(e)

450 (b)(1) Sec 1.7(e)

**SECRET**

**SECRET**

453 (2) (U) (b)(1) Sec 1.7(e)

454 (b)(1) Sec 1.7(e)

455 (3) (U) (b)(1) Sec 1.7(e)

456 (b)(1) Sec 1.7(e)

458 (4) (U) (b)(1) Sec 1.7(e)

459 (b)(1) Sec 1.7(e)

461 (5) (U) Counterintelligence (CI). See Appendix 3 (Counterintelligence).

462 (6) (U) Other Collection Activities. None.

463 f. (U) Processing and Evaluation. See the NISP and (b)(1) Sec 1.7(e)

464 (b)(1) Sec 1.7(e)

465 g. (~~S~~//REL USA, AUS, GBR) Analysis and Production. USSTRATCOM/J2

466 (b)(1) Sec 1.4(a)

467 (b)(1) Sec 1.4(a) either a RAC or a CAC for each intelligence task listed

468 in the ITL, were identified based on (b)(1) Sec 1.4(a)

469 and the collection, analysis, and production assessments completed by

470 agencies within DoD Intelligence. Organizations that do not meet the

471 RAC/CAC criteria can be identified as providing "other support capabilities." A

472 RAC is the lead organization responsible for producing the finished intelligence

473 product to the requesting combatant command. The RAC will specify the need

474 for and scope of the support that CACs will provide to the RAC. Each RAC and

475 CAC will update the assessment of their ability to satisfy assigned tasks from

476 the ITL (b)(1) Sec 1.4(a) or

477 when deemed necessary by USSTRATCOM, USD(I), (b)(1) Sec 1.4(a)

478 h. (U) Dissemination and Integration

479 (1) (~~S~~//REL) Reports Required. Reports will differ based on the

480 information contained in (b)(1) Sec 1.4(a)

481 (b)(1) Sec 1.4(a)

482 (2) (~~S~~//REL) Formats. Formats will differ based on the information

483 contained in (b)(1) Sec 1.4(a)

484 (3) (~~S~~//REL USA, AUS, GBR) Distribution. USSTRATCOM uses (b)(1) Sec 1.4(a)

485 (b)(1) Sec 1.4(a) and

486 SIPRNET. Each combatant command will determine dissemination

487 requirements to support execution of its associated cyberspace operations

~~SECRET~~

498 CONPLANs and OPLANs. See the NISP for detailed information on integration  
499 efforts to support cyberspace operations planning and operations.  
500

501 (4) (U) Foreign Disclosure. To the greatest extent possible, all intelligence  
502 reports will be classified as "releasable to" as many allied partners as practical,  
503 especially Great Britain, Canada, and Australia. The combatant command(s)  
504 responsible for executing cyberspace operations will identify disclosure and  
505 intelligence sharing requirements needed to support the specific operations.  
506

507 (5) (U) (b)(1) Sec 1.7(e) [redacted] if  
508 applicable.  
509

510 i. (U) Coordinating Instructions

511 (1) (U) Conferences

512 (a) (U) USSTRATCOM/J2 will host, as required, planning conferences  
513 to address updates to this CONPLAN and the associated IP effort. Attendance  
514 from combatant command J2s, (b)(1) Sec 1.7(e)  
515 [redacted]  
516 (b)(1) Sec 1.7(e)  
517 [redacted]

518 USSTRATCOM/J2 will send the announcement via message traffic and other  
519 means to ensure widest possible information dissemination (e.g., e-mail, JWICS  
520 and SIPRNET web pages, Secure Video Teleconference (SVTC) sessions, etc.).  
521 (b)(1) Sec 1.7(e)  
522 [redacted]  
523

524 (b) (U) USSTRATCOM components and centers may host intelligence  
525 planning conferences to support specific USSTRATCOM or combatant  
526 command planning efforts or to address cyberspace operations related issues  
527 in their specific areas of expertise.  
528

529 (2) (U) See the NISP for specific instructions on DoD, U.S. government  
530 interagency, and multi-national coordinating instructions.  
531

532 (U)(3) (~~S//REL USA, AUS, GBR~~) USSTRATCOM uses a variety of  
533 collaborative tools to coordinate cyberspace operations activity. SIPRNET is the  
534 preferred collaboration venue to ensure the greatest inclusion of operators,  
535 planners, and intelligence personnel from all echelons of command. The  
536 paragraphs below outline the major cyberspace operations coordination  
537 activities for USSTRATCOM. Although current collaborative tools may change,  
538 the basic functionality will remain and be used in support of mission  
539 objectives.  
540

541 (a) (~~S//REL USA, AUS, GBR~~) SIPRNET (b)(1) Sec 1.4(a)  
542 [redacted]  
543 [redacted]

~~SECRET~~

544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588

(b)(1) Sec 1.4(a)

(U) (b) (~~S//REL USA, AUS, GBR~~) JWICS Page. USSTRATCOM uses the JWICS SKIWeb portal and 8039 IP page for coordination on activities and information dissemination that requires higher classification levels than what is maintained on SIPRNET.

(c) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
USSTRATCOM/ J2 uses (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(d) (U) Secure Video Teleconference (SVTC). USSTRATCOM has a number of (b)(1) Sec 1.7(e) for coordination and collaboration on cyberspace operations activities.

a. (U) Orders to Subordinate and Supporting Units

(1) (U) JFCC-NW

(a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) plan development.

(b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) defense of the DoD Global Information Grid (GIG).

(c) (~~S//REL USA, AUS, GBR~~) Coordinate intelligence collection/ analysis (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) and distribute as required.

(d) (~~S//REL USA, AUS, GBR~~) Coordinate with all other functional component commands for (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(2) (U) JFCC-ISR

(a) (U) Develop, maintain, and update a Global ISR strategy for cyberspace operations and an ISR Functional Support Plan to the NISP within the IP process.

**SECRET**

589 (b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) required  
590 by the CONPLAN 8039 NISP.

591  
592 (3) (U) Joint Functional Component Command for Global Strike and  
593 Integration (JFCC-GSI)

594  
595 (a) (~~S//REL USA, AUS, GBR~~) Coordinate with JFCC-NW for (b)(1) Sec 1.4(a)  
596 (b)(1) Sec 1.4(a)  
597  
598

599 (4) (U) Joint Task Force-Global Network Operations (JTF-GNO)

600  
601 (U)(a) (~~S//REL USA, AUS, GBR~~) Coordinate with USSTRATCOM/J2 for  
602 inclusion of CONPLAN 8039 IP into JTF-GNO planning efforts.

603  
604 (U)(b) (~~S//REL USA, AUS, GBR~~) Provide intelligence support as required  
605 by the CONPLAN 8039 NISP.

606  
607 (c) (~~S//REL USA, AUS, GBR~~) Provide intelligence planning support  
608 and assets as required to JFCC-NW related to (b)(1) Sec 1.4(a)  
609

610 (d). (~~S//REL USA, AUS, GBR~~) Coordinate with JFCC-NW for (b)(1) Sec 1.4(a)  
611 (b)(1) Sec 1.4(a)  
612  
613

614 (e) (~~S//REL USA, AUS, GBR~~) Provide cyberspace (b)(1) Sec 1.4(a)  
615 (b)(1) Sec 1.4(a)  
616  
617

618 (5) (U) Joint Information Operations Warfare Command (JIOWC)

619  
620 (a) (~~S//REL USA, AUS, GBR~~) Provide intelligence planning support as  
621 required to JFCC-NW related to (b)(1) Sec 1.4(a)  
622

623 (b) (~~S//REL USA, AUS, GBR~~) Provide intelligence support as required  
624 to support (b)(1) Sec 1.4(a) and CONPLAN 8039 NISP.  
625

626 (c) (~~S//REL USA, AUS, GBR~~) Coordinate with JFCC-NW for (b)(1) Sec 1.4(a)  
627 (b)(1) Sec 1.4(a)  
628  
629

630 b. (U) Requests to Higher, Adjacent, and Cooperating Units

631  
632 (1) (U) USD(I). USD(I) is responsible for DoD coordination with other  
633 government agencies (OGAs) for intelligence issues. As the synchronizer and  
634 integrator of DoD intelligence support for cyberspace operations,

**SECRET**



635 USSTRATCOM will work through USD(I) for issues requiring support from  
636 OGAs and also with the combatant command J2s for any PN issues.

637  
638 (2) (U) (b)(1) Sec 1.7(e)

639  
640 (a) (U) (b)(1) Sec 1.7(e) IP efforts  
641 (b)(1) Sec 1.7(e) IP process with other  
642 active IP efforts.

643  
644 (b) (U) (b)(1) Sec 1.7(e)  
645 (b)(1) Sec 1.7(e)

646  
647  
648 (c) (U) Lead development of the NISP in support of the IP; (b)(1) Sec 1.7(e)  
649 (b)(1) Sec 1.7(e)  
650  
651 enable the IP to function as a whole.

652  
653 (d) (U) (b)(1) Sec 1.7(e)  
654 (b)(1) Sec 1.7(e)

655  
656 (e) (U) (b)(1) Sec 1.7(e)  
657 (b)(1) Sec 1.7(e)

658  
659 (f) (U) (b)(1) Sec 1.7(e)  
660 (b)(1) Sec 1.7(e)

661  
662  
663 (g) (U) (b)(1) Sec 1.7(e)

664  
665 (3) (U) Joint Staff (b)(1) Sec 1.7(e)

666  
667 (a) (U) Develop (b)(1) Sec 1.7(e) in support of cyberspace  
668 operations.

669  
670 (b) (U) Provide a (b)(1) Sec 1.7(e) to the NISP for this  
671 CONPLAN IP.

672  
673 (4) (U) (b)(1) Sec 1.7(e)

674  
675 (a) (U) (b)(1) Sec 1.7(e)  
676 (b)(1) Sec 1.7(e)

677  
678  
679

**SECRET**

680 (b) (U) Post updated versions of IP products (b)(1) Sec 1.7(e)  
681 (b)(1) Sec 1.7(e)

682  
683 (c) (U) (b)(1) Sec 1.7(e)  
684 (b)(1) Sec 1.7(e)

685  
686 (d) (U) Provide support as required by the CONPLAN 8039 NISP.

687  
688 (5) (U) (b)(1) Sec 1.7(e)  
689 (b)(1) Sec 1.7(e)  
690  
691  
692  
693  
694

695 (6) (U) (b)(1) Sec 1.7(e)

696  
697 (a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
698 (b)(1) Sec 1.4(a) CONPLAN 8039 ITL.

699  
700 (b) (~~S//REL USA, AUS, GBR~~) Coordinate, as appropriate for  
701 (b)(1) Sec 1.4(a)  
702  
703  
704  
705

706 (7) (U) GCC J2s

707  
708 (U)(a) (~~S//REL USA, AUS, GBR~~) Provide cyberspace-related intelligence  
709 requirements for inclusion into the CONPLAN 8039 ITL.

710  
711 (b) (~~S//REL USA, AUS, GBR~~) Coordinate, as appropriate for  
712 cyberspace operations issues, with USSTRATCOM/J2 to ensure  
713 synchronization between the respective GCC's plans and CONPLAN 8039, to  
714 (b)(1) Sec 1.4(a) for  
715 cyberspace operations intelligence requirements.

716  
717 (8) (U) USJFCOM/J2

718  
719 (a) (U) Work with (b)(1) Sec 1.7(e) USSTRATCOM, and the GCCs to develop  
720 an (b)(1) Sec 1.7(e)

721  
722 (b) (U) Develop procedures and training to support (b)(1) Sec 1.7(e)  
723 intelligence and the IP process in support of this CONPLAN 8039.

724  
725 (c) (U) Develop modeling and simulation of processes in the IP process.

**SECRET**

726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765

(d) (U) Develop modeling against (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

(e) (U) Develop an automated (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) IPs.

c. (U) Shortfalls and Limiting Factors

(1) (U) The Services, Combatant Commands, and Agencies often (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

(2) (S) Intelligence community (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

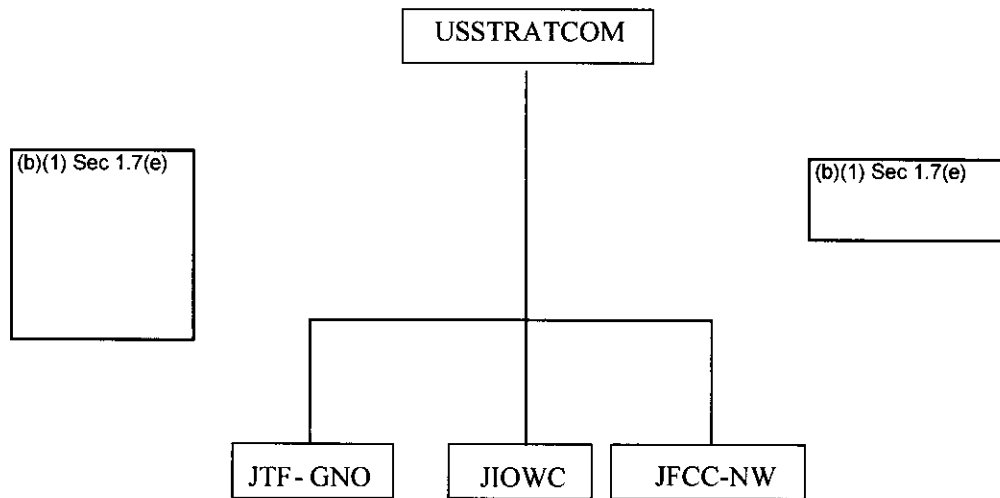
d. (~~S~~//~~REL USA, AUS, GBR~~) Miscellaneous. Combatant commands, CSAs, Service intelligence centers, and USSTRATCOM components may evaluate the effectiveness of CONPLAN 8039 and this IP effort and forward any requests or recommendations to USSTRATCOM/J2 for improvements to this Annex, the (b)(1) Sec 1.4(a)

4. Administration and Logistics N/A

5. Command and Control

a. (U//~~FOUO~~) Intelligence Relationships. USSTRATCOM HQ and each JFCC, Center, and JTF have organic intelligence capabilities. Each provides tailored application of intelligence to satisfy respective commanders' requirements by minimizing duplication and maximizing integration.

(1) (U//~~FOUO~~-) USSTRATCOM/J2. Provides strategic-level intelligence support to the HQ and components. HQ J2 leverages authorities and resources to ensure effective intelligence support across the USSTRATCOM intelligence enterprise, while facilitating collaboration between mission partners and the integration and synchronization of intelligence needs. HQ J2 is organized to provide intelligence planning (IP) effort in support of command planning activities. Figure 1 shows a high level representation of the command relationships with key organizations relating to cyberspace operations.



— Direct Relationship  
 - - - - - Supporting Relationship

Figure 1 – (U) Command Relationships

766  
 767  
 768  
 769  
 770  
 771  
 772  
 773  
 774  
 775  
 776  
 777  
 778  
 779  
 780  
 781  
 782  
 783  
 784  
 785  
 786  
 787  
 788  
 789  
 790  
 791  
 792  
 793  
 794  
 795

(2) (U) (b)(1) Sec 1.7(e)  
 (b)(1) Sec 1.7(e)

(3) (U) Joint Task Force-Global Network Operations J2 (JTF-GNO/J2). Provides tailored intelligence in support of the operation and defense of the GIG, including DoD-wide computer network defense (b)(1) Sec 1.7(e)  
 (b)(1) Sec 1.7(e)  
 business missions. The JTF-GNO/J2 provides timely and relevant intelligence to the Commander, Joint Task Force – Global Network Operations, JTF Staff, and components through (b)(1) Sec 1.7(e)  
 (b)(1) Sec 1.7(e)  
 (b)(1) Sec 1.7(e) in support of the operation and defense of the Global Information Grid.

(4) (U) Joint Information Operations Warfare Command J2 (JIOWC/J2). Focal point for intelligence support to information operations within the JIOWC. JIOWC/J2 coordinates directly with combatant command and JTF intelligence entities, to include Joint Intelligence Operation Centers. JIOWC/J2 provides (b)(1) Sec 1.7(e)  
 (b)(1) Sec 1.7(e)

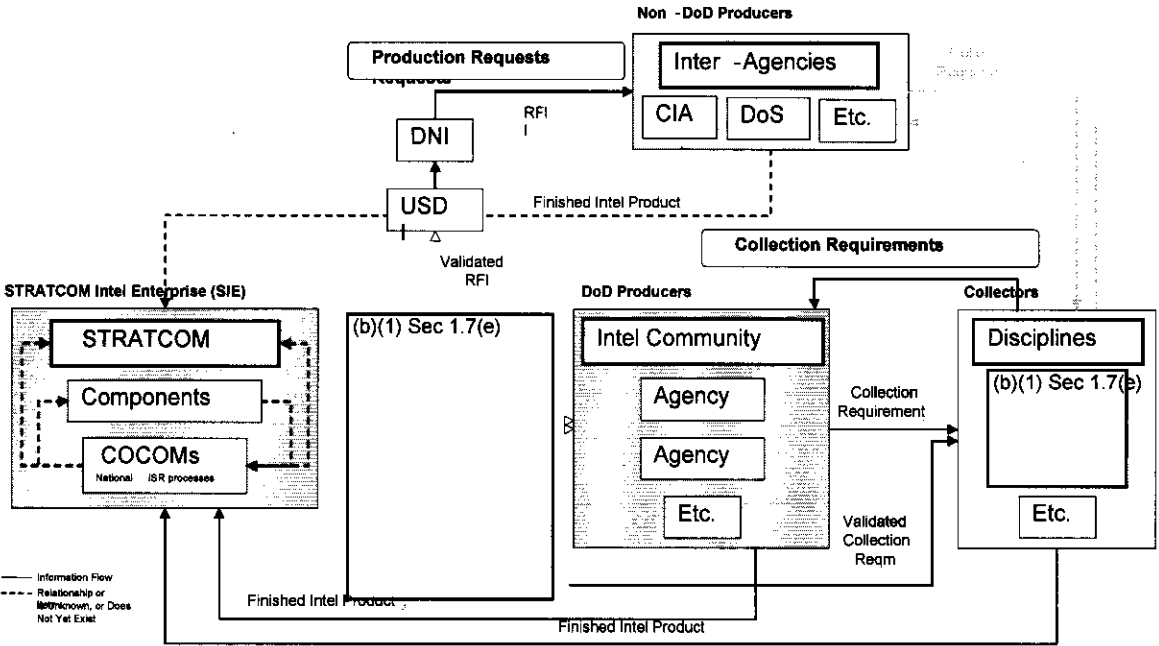
796 Additionally, the JIOWC/J2 assists (b)(1) Sec 1.7(e)  
797 (b)(1) Sec 1.7(e)

798  
799 (5) (U) Joint Functional Component Command-Network Warfare J2  
800 (JFCC-NW/J2). Provides intelligence to support the optimization of planning,  
801 integration, coordination, execution, and force management of the Network  
802 Warfare missions in support of joint warfighters. In coordination with JTF-  
803 GNO, JFCC-NW maintains situational awareness for the DoD GIG while

804 (b)(1) Sec 1.7(e)

805 (b)(1) Sec 1.7(e) In addition to the wide  
806 range of products JFCC-NW provides to support cyberspace operations  
807 planning, (b)(1) Sec 1.7(e)

808  
809 b. (U) Communications. USSTRATCOM/J2, component J2s, and relevant  
810 combatant command J2s make up the USSTRATCOM Intelligence Enterprise  
811 (SIE) to collaborate on intelligence support. The SIE is the customer in Figure  
812 2, and the information exchange between agencies in the cyberspace  
813 environment is depicted in the diagram. The SIE submits a Production  
814 Request (PR) via (b)(1) Sec 1.7(e) The dotted lines within the customer box are to  
815 show that, ideally, each affected member of the SIE should receive a copy of the  
816 PR to ensure receipt of the finished intelligence product.



817  
818 **Figure 2 – (U) Communications and Information Exchange**

819  
820 (1) (U) The PR (b)(1) Sec 1.7(e) to ensure the appropriate  
821 subtasking of PRs to the producer(s). The producer accomplishes the PR and  
822 submits their own collection requirements, if needed, to the appropriate

**SECRET**

823 collector. As mentioned above, the JFCCs have been directed to submit  
824 production requirements directly to the DoD producers. In the case where the  
825 PR and a non-DoD agency meet, the PR is routed through the USD(I) and the  
826 Director of National Intelligence (DNI), assigned to the appropriate non-DoD  
827 producer who may task a collector if needed, and then the finished intelligence  
828 product is routed back to the STRATCOM Intelligence enterprise (SIE). The  
829 process for a non-DoD agency to task a collector is not directed by this  
830 CONPLAN and, therefore, is grayed out in the diagram.

831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859

(2) (U) Collection requirements (CR) that originate from the SIE are  
(b)(1) Sec 1.7(e) prior to fielding by the collectors. The combatant  
command process for tasking national assets follows the path shown in the  
diagram. (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) and ensure appropriate subtasking of  
both PRs and CRs.

**Appendices**

- 1- (b)(1) Sec 1.7(e)
- 2- (b)(1) Sec 1.7(e)
- 3--Counterintelligence (CI)
- 4- (b)(1) Sec 1.7(e)
- 5- (b)(1) Sec 1.7(e)
- 6--Intelligence Support to Information Operations (IO)
- 7- (b)(1) Sec 1.7(e)
- 8-
- 9-

Kevin P. Chilton  
General, USAF  
COMMANDER

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AFB NE 68113-6500  
28 February 2008

1 APPENDIX 1 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)

2 (U) OPR: HQ J2

3 (b)(1) Sec 1.7(e) (U)

4  
5 1. (U) General. (b)(1) Sec 1.7(e) are the basic

6 (b)(1) Sec 1.7(e)  
7  
8

9 requirements to support planning and operations regarding computer network  
10 operations. The (b)(1) Sec 1.7(e)

11 (b)(1) Sec 1.7(e) to support this plan.

12  
13 2. (U) (b)(1) Sec 1.7(e) have been identified for the (b)(1) Sec 1.7(e) CONPLAN 8039

14 execution. Due to the similarity in intelligence requirements for (b)(1) Sec 1.7(e)

15 (b)(1) Sec 1.7(e) will be combined for  
16 these (b)(1) Sec 1.7(e)

17  
18 3. (U) Each (b)(1) Sec 1.7(e) will list the supporting tasks and subtasks that further define  
19 the cyberspace operations intelligence requirements. The (b)(1) Sec 1.7(e) are:

20  
21 a. (U) (b)(1) Sec 1.7(e)

22 (b)(1) Sec 1.7(e)  
23

24 b. (U) (b)(1) Sec 1.7(e)

25 (b)(1) Sec 1.7(e)  
26

27  
28 c. (U) (b)(1) Sec 1.7(e)

29 (b)(1) Sec 1.7(e)  
30  
31

32  
33 d. (U) (b)(1) Sec 1.7(e)

34 (b)(1) Sec 1.7(e)  
35

Classified by: Multiple Sources  
Reason: 1.4(a), (e), and (g)  
Declassify on: 26 February 2008 2032

**SECRET**

36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55

e. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

f. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

g. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) cyberspace  
networks?

Kevin P. Chilton  
General, USAF  
COMMANDER



**SECRET**

HEADQUARTERS, U.S. STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE NE 68113-6500  
28 February 2008

APPENDIX 2 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)

(U) OPR: HQ J2

(b)(1) Sec 1.7(e) (U)

(U) References:

a. (U) (b)(1) Sec 1.7(e), 25 Jan 73  
(S).

b. (U) (b)(1) Sec 1.7(e)  
10 Aug 88 (U).

c. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e), 31 May 01 (U).

d. (U) Joint Pub 2-01, Joint Intelligence Support to Military Operations,  
Appendix C, 26 Aug 02 (S).

e. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e), 12 Jun 95 (U).

f. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) (U // FOUO).

g. (U) (b)(1) Sec 1.7(e)  
June 05 (TS//TK).

h. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e), 1 May 06 (U).

1. (U) Situation. This appendix provides a review of general responsibilities and procedures for submitting (b)(1) Sec 1.7(e) requirements to support planning, (b)(1) Sec 1.7(e) intelligence, readiness, posturing, situational awareness, and mission execution. Additional (b)(1) Sec 1.7(e) capability which may contribute to USSTRATCOM (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) Combatant

Commands and tasked by their respective Service.

~~Classified by: Multiple Sources~~

~~Reason: 1.4(a), (e), and (g)~~

~~Declassify on: 26 February 2008 2032~~

**SECRET**

~~SECRET~~

43 a. (U) (b)(1) Sec 1.7(e) See 8039 Annex B (Intelligence) (b)(1) Sec 1.7(e)

44 (b)(1) Sec 1.7(e)

45  
46 b. (U) Friendly. Refer to Base Plan.

47  
48 c. (U) Assumptions. Refer to Base Plan.

49  
50 d. (U) Legal Considerations. Refer to Base Plan and Annex B (Intelligence).

51  
52 e. (U) Collection Priorities

53  
54 (1) (U) Priority 1 through Priority 7. Not applicable.

55  
56 (2) (U) (b)(1) Sec 1.7(e) USSTRATCOM/J2 Requirements

57 (b)(1) Sec 1.7(e)

support to HQs staff elements.

58 USSTRATCOM Joint Functional Component Commands (JFCCs), components,

59 and subordinate commands manage cyber operations (b)(1) Sec 1.7(e)

60 functions for their organizations." JFCC-Intelligence, Surveillance, and

61 Reconnaissance (JFCC-ISR)"" (b)(1) Sec 1.7(e)

62 (b)(1) Sec 1.7(e)

63  
64  
65  
66  
67 (3) (U) (b)(1) Sec 1.7(e)

68 (b)(1) Sec 1.7(e)

69  
70  
71  
72  
73  
74 (a) (U) Conduct all-source intelligence analysis/assessments.

75  
76 (b) (U) Support command components and assigned units.

77  
78 (c) (U) Support real-time global cyber operations and intelligence

79 decision-making.

80  
81 (d) (U) Support Commander, USSTRATCOM, in operations to support

82 the President of the United States, the Secretary of Defense (SecDef), and other

83 Unified Commanders.

84  
85 2. (U) Mission. Refer to Base Plan.

86  
87 3. (U) Execution. Refer to Annex B (Intelligence), para. 3.

88

~~SECRET~~

89 a. (U) Concept of Operations

90  
91 (1) (U) (b)(1) Sec 1.7(e) Organizations

92  
93 (a) (S//REL) (b)(1) Sec 1.4(a)

94 (b)(1) Sec 1.4(a)  
95  
96  
97  
98  
99  
100  
101

102 (b) (U) The (b)(1) Sec 1.7(e)

103 (b)(1) Sec 1.7(e)  
104  
105  
106  
107

108 (c) (U) (b)(1) Sec 1.7(e)

109 (b)(1) Sec 1.7(e)  
110  
111

113 (d) (U) (b)(1) Sec 1.7(e) provide timely, responsive processing and validation of  
114 USSTRATCOM (b)(1) Sec 1.7(e)

115 (b)(1) Sec 1.7(e) feedback on the status of  
116 requirements.

117  
118 b. (U) Responsibilities

119  
120 (1) (U) JFCC-NW. Provide timely submission for (b)(1) Sec 1.7(e)  
121 needs in support of this CONPLAN. Maintain all appropriate tabs to this  
122 appendix.

123  
124 (2) (U) (b)(1) Sec 1.7(e)

125  
126 (a) (U) (b)(1) Sec 1.7(e)

127 (b)(1) Sec 1.7(e)

128  
129 (b) (U) (b)(1) Sec 1.7(e)

130 (b)(1) Sec 1.7(e)  
131  
132  
133

134 (c) (U) (b)(1) Sec 1.7(e)  
135 (b)(1) Sec 1.7(e)  
136  
137  
138

139 (d) (U) (b)(1) Sec 1.7(e)  
140 (b)(1) Sec 1.7(e)  
141  
142  
143

144 (3) (U) (b)(1) Sec 1.7(e)

145  
146 (a) (U) (b)(1) Sec 1.7(e)  
147 (b)(1) Sec 1.7(e)

148  
149 (b) (U) (b)(1) Sec 1.7(e)  
150 (b)(1) Sec 1.7(e)

151  
152 (c) (U) (b)(1) Sec 1.7(e)  
153 (b)(1) Sec 1.7(e)  
154  
155

156  
157 (d) (U) (b)(1) Sec 1.7(e)  
158 (b)(1) Sec 1.7(e)

159  
160 c. (U) Tasks. Refer to Annex B (Intelligence).

161  
162 d. (U) Coordinating Instructions. Refer to Annex B (Intelligence).

163  
164 4. (U) Administration and Logistics. Not Applicable.

165  
166 5. (U) Command and Control

167  
168 a. Command and Control. Refer to Annex J (Command Relationships).

169  
170 b. Communications Systems. Refer to Annexes B (Intelligence) and K (C4  
171 Systems).

172  
173  
174 Kevin P. Chilton  
175 General, USAF  
176 COMMANDER

~~SECRET~~

HEADQUARTERS, U.S. STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE NE 68113-6500  
28 February 2008

1 APPENDIX 3 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)

2 (U) OPR: HQ J2

3 COUNTERINTELLIGENCE (CI) (U)

4  
5 (U) References:

6  
7 a. (U) Executive Order 12333, United States Intelligence Activities, 4 Dec 81  
8 (U).

9  
10 b. (U) DOD Regulation 5200.1-R, Information Security Program Regulation,  
11 Jan 97 (U).

12  
13 c. (U) DOD Directive 5105.67, Dept of Defense Counterintelligence Field  
14 Activity, 19 Feb 02. (U)

15  
16 d. (U) DOD Directive 5200.27, Acquisition of Information Concerning  
17 Persons and Organizations not Affiliated with the Department of Defense, 7 Jan  
18 80 (U).

19  
20 e. (U) DOD Directive 5240.1, DOD Intelligence Activities, 25 Apr 88 (U).

21  
22 f. (U) DOD Regulation 5240.1R, Procedures Governing the Activities of DOD  
23 Intelligence Components that Affect United States Persons, Dec 82 (U).

24  
25 g. (U) DOD Directive 5240.2, DOD Counterintelligence, 22 May 97 (U).

26  
27 h. (U) DOD Instruction 5240.4, Reporting of CI and Criminal Violations, 22  
28 Sep 92, w/Ch 1, 8 Apr 92 (U).

29  
30 i. (U) DOD Instruction 5240.8, Security Classification Guide for Information  
31 Concerning the DOD Counterintelligence Program (U) ASD(NII), 16 Nov 00 (C).

32  
33 j. (U) DOD Instruction C-5240.10, Counterintelligence Support to the  
34 Combatant Commands and the Defense Agencies, 14 May 04 (U).

35  
36 k. (U) (b)(1) Sec 1.7(e)  
37 (b)(1) Sec 1.7(e) (U).

38  
~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (e), and (g)~~  
~~Declassify on: 26 February 2032~~

~~SECRET~~

B-3-1

**SECRET**

39 1. (U//~~FOUO~~) Office of the Under Secretary of Defense, Deconfliction of  
40 DOD Counterintelligence (CI) Cyber Operations with the Intelligence  
41 Community (IC) (U//~~FOUO~~), 2 Feb 07.

42  
43 1. (U) Situation

44  
45 a. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

46 (b)(1) Sec 1.4(a) US IO; C4ISR; critical infrastructure; and cyberspace-  
47 related systems, technologies, facilities, and resources exist. (b)(1) Sec 1.4(a)

48 (b)(1) Sec 1.4(a)  
49  
50  
51  
52  
53  
54  
55  
56  
57

58 (b)(1) Sec 1.4(a) Refer to Annex B of Base Plan for current  
59 overarching threat information and (b)(1) Sec 1.4(a)

60 (b)(1) Sec 1.4(a)

61  
62 b. (U) Friendly

63  
64 (1) (U) US National Agencies. Prior to, during, and following execution of  
65 any portion of this plan, CI, law enforcement, security, or intelligence support  
66 may be requested of the following organizations: DHS; Department of Justice  
67 (DOJ), including the Federal Bureau of Investigation (FBI); Central Intelligence  
68 Agency (CIA); NSA; DIA; National Counterintelligence Executive (NCIX); U.S.  
69 Marshals Service (USMS); CIFA; the Service CI, law enforcement, and security  
70 organizations, including AFOSI, NCIS, U.S. Army INSCOM, U.S. Marine Corps  
71 CI, United States Coast Guard (USCG) CI, and the U.S. Army CID; and various  
72 state-level departments, such as the National Guard and state and local police.

73  
74 (a) (U) USSTRATCOM/Counterintelligence Staff Office (CISO) will serve  
75 as the focal point for integrating, synchronizing, and coordinating all  
76 USSTRATCOM CONPLAN 8039-related CI activities.

77  
78 (b) (U) The U.S. Air Force, Army, Navy, and Marine Corps CI elements  
79 will provide CI support to their respective Services in support of the  
80 USSTRATCOM mission.

81  
82 (c) (~~S//REL USA, AUS, GBR~~) Each tasked CI organization will

83 (b)(1) Sec 1.4(a)

**SECRET**

84 (b)(1) Sec 1.4(a)  
85 (b)(1) Sec 1.4(a) with USSTRATCOM CISO.

86  
87 (2) (U) Command CI Structure. Upon execution of CONPLAN 8039, the  
88 USSTRATCOM CISO (b)(1) Sec 1.7(e)  
89 (b)(1) Sec 1.7(e) and will perform associated duties in coordination with  
90 affected geographic combatant command/functional combatant command  
91 CISOs and designated Task Force CI Coordinating Authorities (TFCICAs).

92  
93 (a) (U) USSTRATCOM CISO is responsible to plan, coordinate,  
94 advocate, and integrate the overall collaborative CI effort in support of this  
95 plan. Unless execution authority is transferred to another combatant  
96 commander, CDRUSSTRATCOM is the supported Commander. USSTRATCOM  
97 CISO is the CI representative for CDRUSSTRATCOM.

98  
99 (b) (U) If another combatant commander is designated the supported  
100 Commander under this plan, that command's CISO becomes responsible for all  
101 planning, coordination, and integration of CI support to this plan and  
102 USSTRATCOM CISO becomes a supporting CI element. Supported combatant  
103 command CISO will designate a TFCICA.

104  
105 (c) (~~S//REL USA, AUS, GBR~~) All combatant command CISOs and  
106 Service CI agencies will ensure the supported TFCICA receives, in a timely  
107 manner, (b)(1) Sec 1.4(a)

108 (b)(1) Sec 1.4(a)  
109  
110  
111  
112 information copies of all CI planning, coordination, (b)(1) Sec 1.4(a)

113  
114 (d) (U) The respective Service and its CI organizational headquarters  
115 will exercise operational control over its Military Department CI resources,  
116 unless specified otherwise by legal authority.

117  
118 (e) (U) Administrative control of Military Department CI resources  
119 remains with the CI organization of the respective Service.

120  
121 (f) (U) Assigned and supporting CI assets will utilize all available CI  
122 activities to support this plan. CI activities include all (b)(1) Sec 1.7(e)  
123 (b)(1) Sec 1.7(e) available within CI investigations, operations, collections, and  
124 analysis and production.

125  
126 (g) (U) All CI information relative to this plan will be made known to  
127 USSTRATCOM Commander and the supported Commander through the  
128 Commander's CISO or other CI element, if so named. CI information will be  
129 shared through the most expeditious means available.

**SECRET**

**SECRET**

130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175

(3) (U) Allied. Allied and coalition elements provide support based on national plans and agreements.

c. (U) Assumptions

(1) (U) The supported CISO, when required, will serve as or appoint a TFCICA. The TFCICA will establish CI reporting channels and requirements with component and other agency CI organizations upon implementation or execution of this plan.

(2) (U) All command elements and components will have dedicated CI support.

(3) (U) Components and national support agencies will provide pre-execution and post-execution CI support and services.

(4) (U) All CI organizations will follow appropriate US laws, directives, regulations, and policies regarding CI activities that involve US persons, enemy prisoners of war, and the LOAC.

2. (U) Mission. See Base Plan.

3. (U) Execution

a. (~~S//REL USA, AUS, GBR~~) Concept of Operations. The integration and synchronization of CI in support of this CONPLAN is the responsibility of CISO. Upon implementation of this CONPLAN, the CISO assumes the roles and responsibilities of the

(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(1) (~~S//REL USA, AUS, GBR~~) Information collection and protection

(b)(1) Sec 1.4(a)

(2) (U) The discharge of special CI requirements assigned by higher authority, e.g., USD(I), CJCS, etc.

(3) (U) Supporting Service CI elements will accomplish CI missions within respective jurisdictions in accordance with established Service policies and



**SECRET**

176 procedures. Assigned CI elements will be guided by applicable DOD, Joint  
177 Staff, or combatant command policies and procedures. All Service CI elements  
178 will provide information and coordination copies of Service-unique field CI

179 (b)(1) Sec 1.7(e)

182 activities that are supporting this CONPLAN.

184 b. (U) Tasks

186 (1) (U) Counterintelligence Collection and Reporting

188 (a) (U) Service CI Elements. Forward Service-unique field CI  
189 collections and standard (b)(1) Sec 1.7(e)

190 (b)(1) Sec 1.7(e)

192 (b) (U) (b)(1) Sec 1.7(e)

193 (b)(1) Sec 1.7(e)

195 (c) (U) USSTRATCOM (b)(1) Sec 1.7(e) CISO

197 (1) (U) Develop CI collection requirements specific to USSTRATCOM  
198 and in coordination with JFCC NW, JTF GNO, and other affected combatant  
199 commands/agencies.

201 (2) (U) Ensure all products generated in support of this plan are  
202 distributed to Commander USSTRATCOM, JFCC NW, JTF GNO, Joint Staff/J2,  
203 other combatant commands and task forces as appropriate.

205 (3) (U) Coordinate CI collection activities and maintain liaison with  
206 national level CI and law enforcement agencies as well as other affected  
207 COCOM CISOs.

209 (4) (U) Coordinate with national level agencies for collection,  
210 analysis, and production in support of critical mission needs.

212 (2) (U) Counterintelligence Analysis and Production. See para. 3.b.(1),  
213 above.

215 (3) (U) Counterintelligence Investigations. Investigations will be  
216 conducted by the military services and/or the appropriate national agencies.  
217 Services will brief CDRUSSTRATCOM through the CISO (b)(1) Sec 1.7(e)  
218 (b)(1) Sec 1.7(e) affecting this CONPLAN.

220 (4) (~~C//REL~~) Counterintelligence Operations. Individual Service  
221 components and/ or appropriate national agencies (b)(1) Sec 1.4(a)

**SECRET**

SECRET

222 (b)(1) Sec 1.4(a) activities as directed or required in support of this  
223 CONPLAN. Services will brief CDRUSSTRATCOM through the  
224 CISO (b)(1) Sec 1.4(a) operations and activities affecting this  
225 CONPLAN.  
226

227 (5) (U) Functional Services. Individual service components and/or  
228 appropriate national agencies will conduct CI functional services as required by  
229 this CONPLAN. Services will brief CDRUSSTRATCOM through the  
230 CISO (b)(1) Sec 1.7(e) on the overall status of functional services activities.  
231

232 c. (U) Coordinating Instructions. All higher, lateral, and subordinate  
233 Service and DOD level CI elements will keep the USSTRATCOM CISO/  
234 (b)(1) Sec 1.7(e) as appropriate, of  
235 their CI operations and activities. USSTRATCOM CISO (b)(1) Sec 1.7(e)  
236 (b)(1) Sec 1.7(e) in  
237 support of this CONPLAN. These roles and responsibilities (b)(1) Sec 1.7(e)  
238 (b)(1) Sec 1.7(e)  
239

241 4. (U) Administration and Logistics. USSTRATCOM CISO (b)(1) Sec 1.7(e)  
242 manages the Command's CI program. In this role, the USSTRATCOM CI Staff  
243 Office will assist the component's CI services in coordinating their activities  
244 and to identify Service-specific requirements. New CI requirements should be  
245 forwarded to USSTRATCOM CISO (b)(1) Sec 1.7(e)  
246 USSTRATCOM CI Staff Office coordinates with USSTRATCOM (b)(1) Sec 1.7(e)  
247 (b)(1) Sec 1.7(e) as required,  
248 to satisfy CI requirements in support of USSTRATCOM (b)(1) Sec 1.7(e)  
249

250 5. (U) Command and Control

251  
252 a. (U) Command Relationships. This CONPLAN does not require an  
253 assumption of OPCON or TACON of Service CI elements. Commander,  
254 USSTRATCOM, through the CISO (b)(1) Sec 1.7(e) exercises staff coordination  
255 authority over supporting Service CI elements. If CDRUSSTRATCOM cannot  
256 obtain necessary agreement on an issue, CDRUSSTRATCOM will request  
257 resolution of the issue from the Director of CI, Deputy Assistant Secretary of  
258 Defense for Counterintelligence & Security, through the CJCS. Such requests  
259 will be forwarded via the JCID, to CJCS. Military Department/Service CI units  
260 designated to support operations retain their command and organizational  
261 integrity. Administrative control also remains with the CI organization of each  
262 Military Department/Service. CI units are responsible for supporting their  
263 Services and responding to CISO (b)(1) Sec 1.7(e) requests for support and  
264 coordination. All CI activity will be conducted in conformity with legal and  
265 policy restrictions regarding CI activities (b)(1) Sec 1.7(e)  
266

**SECRET**

267 b. (U) Command, Control, Communications, Computers, and Intelligence  
268 (C4I). Reporting will be in accordance with established Service procedures and  
269 channels and in message format. Message traffic will be addressed to  
270 USSTRATCOM OFFUTT AFB NE// for (b)(1) Sec 1.7(e) or SSOSTRATCOM//J2// for  
271 (b)(1) Sec 1.7(e)

272  
273  
274  
275  
276

277 Tabs:

- 278 A - (U) Counterintelligence (CI) Target List – Not used.
- 279 B - (U) (b)(1) Sec 1.7(e)
- 280 (b)(1) Sec 1.7(e) USSC
- 281 C - (U) Umbrella CI Force Protection Source Operation Proposal – Not used.

282  
283  
284  
285  
286  
287

288 Kevin P. Chilton  
289 General, USAF  
290 COMMANDER

~~SECRET~~

(INTENTIONALLY BLANK)

~~SECRET~~

B-3-8

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
28 February 2008

APPENDIX 4 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)

(U) OPR: JFCC NW J2

(b)(1) Sec 1.7(e) (U)

(U) References. Refer to Base Plan.

a. (U) (b)(1) Sec 1.7(e) 20  
Mar 2006 (S).

b. (U) (b)(1) Sec 1.7(e) 13 Apr 2007 (U).

1. (~~S//REL USA, AUS, GBR~~) Situation. This appendix provides a review of general responsibilities and procedures for (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

a. (U) (b)(1) Sec 1.7(e) Refer to Annexes B (Intelligence) and (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

b. (U) Friendly. Refer to Base Plan.

c. (U) Assumptions. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

a. a. (~~C//REL~~) (b)(1) Sec 1.4(a) HQ  
USSTRATCOM/J2 will coordinate all (b)(1) Sec 1.4(a)  
USSTRATCOM JFCCs and subordinate commands will manage (b)(1) Sec 1.4(a) for their  
organizations and manage/coordinate (b)(1) Sec 1.4(a) conducted by assigned intelligence  
analysts. Individual USSTRATCOM components will manage (b)(1) Sec 1.4(a) for their specific  
operating environment in coordination with HQ USSTRATCOM/J2, other  
USSTRATCOM components, other COCOM/J2s, (b)(1) Sec 1.4(a) other USG agencies, and

~~Classified by: Multiple Sources  
Reason: 1.4(a), (c), and (g)  
Declassify on: 06 December 2032~~

the IC. DOD Component J2 (b)(1) Sec 1.4(a) elements will coordinate and/or assist

SECRET

38 with (b)(1) Sec 1.4(a) among other  
39 things:

40  
41 (1) (U) Determine (b)(1) Sec 1.7(e) at strategic, operational,  
42 and tactical levels.

43  
44 (2) (U) Identify the (b)(1) Sec 1.7(e)  
45 (b)(1) Sec 1.7(e)

46  
47 (3) (U) Project how the (b)(1) Sec 1.7(e)

48  
49 (4) (~~S//REL USA, AUS, GBR~~) Review Intelligence, Surveillance and  
50 Reconnaissance (ISR) (b)(1) Sec 1.4(a)

51  
52 b. (~~C//REL~~) (b)(1) Sec 1.4(a), USSTRATCOM/J5 will  
53 lead, record, coordinate and update CDR USSTRATCOM (b)(1) Sec 1.4(a)  
54 (b)(1) Sec 1.4(a) Individual USSTRATCOM component J5 elements will record,  
55 validate, coordinate, and update (b)(1) Sec 1.4(a)  
56 (b)(1) Sec 1.4(a) In addition, HQ USSTRATCOM/J5 will coordinate with all  
57 involved (b)(1) Sec 1.4(a)  
58 related to the plan. Individual USSTRATCOM/J5 elements will perform the same  
59 function at the component level related to supporting plans. HQ USSTRATCOM/J5  
60 (b)(1) Sec 1.4(a)  
61 (b)(1) Sec 1.4(a) Individual USSTRATCOM/J5  
62 elements will perform the same function at the component level. DOD Components  
63 and JIATF members will maintain and share cyberspace situational awareness.

64  
65 (1) (U) Component SJA elements will maintain approved Supplemental Rules  
66 of Engagement.

67  
68 (2) (U) Component J5 elements will maintain respective (b)(1) Sec 1.7(e)  
69 (b)(1) Sec 1.7(e)

70  
71 (3) (U) Component J5 elements, supported by their respective J2 elements,  
72 (b)(1) Sec 1.7(e)  
73  
74  
75  
76 USSTRATCOM organizational oversight.

77  
78 c. (U) (b)(1) Sec 1.7(e)

79  
80 (1) (~~C//REL~~) (b)(1) Sec 1.4(a)  
81 (b)(1) Sec 1.4(a) elements responsible  
82 for the (b)(1) Sec 1.4(a) Traditionally,  
83 external organizations conduct the majority of (b)(1) Sec 1.4(a)

SECRET

**SECRET**

84 (b)(1) Sec 1.4(a) JFC staff. However, (b)(1) Sec 1.4(a)  
85 procedures and the scarcity and dispersion of cyber space (b)(1) Sec 1.4(a)  
86 (b)(1) Sec 1.4(a)  
87  
88  
89

90  
91 (2) (C//REL) At any time, any agency may (b)(1) Sec 1.4(a)  
92 (b)(1) Sec 1.4(a)  
93  
94  
95  
96

97  
98 (a) (U) (b)(1) Sec 1.7(e) the best opportunity for recommendations  
99 to (b)(1) Sec 1.7(e) include:

100  
101 1. (U) (b)(1) Sec 1.7(e)

102 (b)(1) Sec 1.7(e)

103  
104 2. (U) LOAC, ROE, or treaty considerations

105  
106 3. (U) (b)(1) Sec 1.7(e)

107 (b)(1) Sec 1.7(e)

108  
109 4. (U) Intelligence (b)(1) Sec 1.7(e)

110  
111 5. (U) (b)(1) Sec 1.7(e)

112  
113 6. (U) (b)(1) Sec 1.7(e)

114  
115 7. (U) (b)(1) Sec 1.7(e)

116  
117 8. (U) To deconflict with friendly operations

118  
119 (b) (C//REL) Component (b)(1) Sec 1.4(a) will maintain the authoritative

120 (b)(1) Sec 1.4(a)  
121  
122

123 (3) (U) Component (b)(1) Sec 1.7(e) elements will request approval via JS (b)(1) Sec 1.7(e) the

124 (b)(1) Sec 1.7(e) thresholds or  
125 ROE.

126  
127 d. (U) Capabilities Analysis. Under the oversight and direction of STRATCOM J2,  
128 component (b)(1) Sec 1.7(e) and J8 elements will determine asset capability and availability,  
129 and, in coordination with individual component J2 and SJA, will estimate (b)(1) Sec 1.7(e)

**SECRET**

SECRET

130 (b)(1) Sec 1.7(e) Individual components and mission partners will consider (b)(1) Sec 1.7(e)

131 (b)(1) Sec 1.7(e)  
132  
133

134  
135 e. (U) Commander's Decision and Force Assignment

136  
137 (1) (C//REL) Component (b)(1) Sec 1.4(a) will establish (b)(1) Sec 1.4(a)  
138 (b)(1) Sec 1.4(a) to present (b)(1) Sec 1.4(a) for approval.

139  
140 (2) (U) (b)(1) Sec 1.7(e) will match their  
141 components' (b)(1) Sec 1.7(e)  
142 (b)(1) Sec 1.7(e) This action will take into account the results of  
143 capabilities analysis as well as (b)(1) Sec 1.7(e)

144 (b)(1) Sec 1.7(e)  
145  
146  
147

148  
149 (3) (C//REL) (b)(1) Sec 1.4(a)  
150 available will (b)(1) Sec 1.4(a)  
151 (b)(1) Sec 1.4(a) as soon as possible in a subsequent (b)(1) Sec 1.4(a)

152  
153 f. (U) Mission Planning and (b)(1) Sec 1.7(e) Component J3s will ensure tasked  
154 units (b)(1) Sec 1.7(e) IAW the applicable  
155 (b)(1) Sec 1.7(e)

156  
157 g. (C//REL) (b)(1) Sec 1.4(a) In coordination with component J3s, (b)(1) Sec 1.4(a)  
158 (b)(1) Sec 1.4(a)

159  
160 h. (C) (b)(1) Sec 1.4(a) If operations (b)(1) Sec 1.4(a)  
161 (b)(1) Sec 1.4(a) will modify this  
162 Appendix and other documents to incorporate (b)(1) Sec 1.4(a)  
163 (b)(1) Sec 1.4(a) associated with (b)(1) Sec 1.4(a)  
164 provide enough data to (b)(1) Sec 1.4(a)

165 (b)(1) Sec 1.4(a)  
166

167  
168 i. (S//REL USA, AUS, GBR) Definitions

169 (1) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
170 (b)(1) Sec 1.4(a) USSTRATCOM is defined as (b)(1) Sec 1.4(a)  
171 (b)(1) Sec 1.4(a)

172  
173  
174



175 by the commander through (b)(1) Sec 1.4(a)  
176 including (b)(1) Sec 1.4(a) This  
177 knowledge of the (b)(1) Sec 1.4(a)

178 (b)(1) Sec 1.4(a) permits commanders to (b)(1) Sec 1.4(a)  
179 (b)(1) Sec 1.4(a)  
180  
181  
182  
183  
184

185 (2) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
186 (b)(1) Sec 1.4(a)  
187 (b)(1) Sec 1.4(a)

188 (3) (S//REL USA, AUS, GBR) Situational Awareness (SA). This activity  
189 encompasses (b)(1) Sec 1.4(a)  
190 (b)(1) Sec 1.4(a)  
191 (b)(1) Sec 1.4(a) all echelons of the chain of  
192 command establish and maintain an understanding of the (b)(1) Sec 1.4(a)  
193 (b)(1) Sec 1.4(a)  
194  
195  
196

197 (4) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
198 (b)(1) Sec 1.4(a)  
199  
200  
201

202 j. (S//REL USA, AUS, GBR) Coordinating Instructions. (b)(1) Sec 1.4(a) should  
203 compare and evaluate the merit (b)(1) Sec 1.4(a)  
204 (b)(1) Sec 1.4(a)  
205  
206

207 4. (U) Administration and Logistics. Refer to Base Plan.

208  
209 5. (U) Command and Control. Refer to Base Plan, Annexes J (Command and Control)  
210 and K (C4 Systems).

211  
212 (b)(1) Sec 1.4(a)

**SECRET**

(b)(1) Sec 1.4(a)

**SECRET**

B-4-6

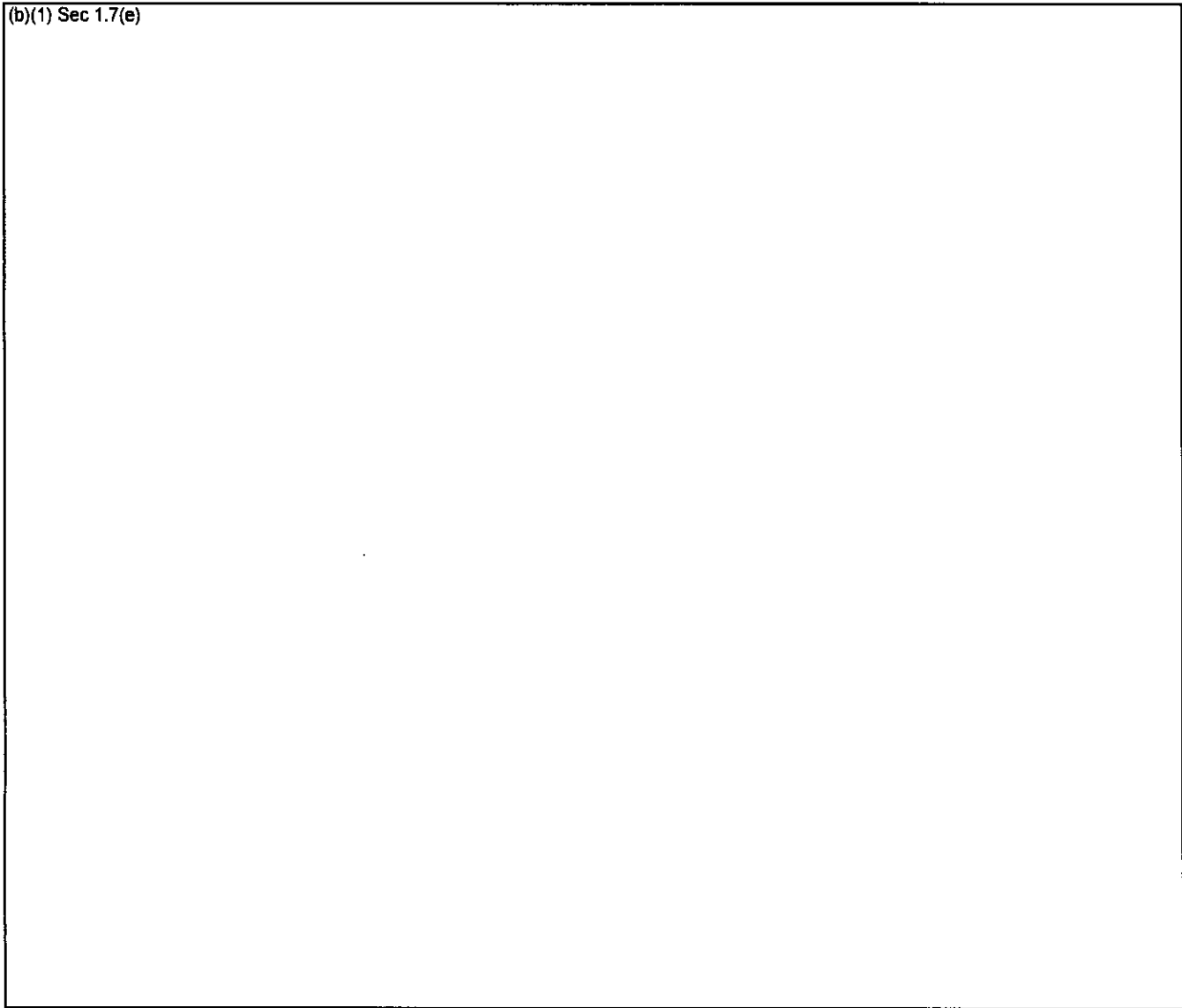
(b)(1) Sec 1.4(a)



213  
214  
215

Figure B-4-1 (b)(1) Sec 1.4(a) (S//REL USA, AUS, GBR)

(b)(1) Sec 1.7(e)



216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229

Figure B-4-2 (b)(1) Sec 1.7(e) (U//FOUO)

Kevin P. Chilton  
General, USAF  
COMMANDER

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
28 February 2008

1  
2 APPENDIX 5 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)

3 (U) OPR: HQ J2

4 (b)(1) Sec 1.7(e) (U)

5  
6 (U) References:

7  
8 a. (U) (b)(1) Sec 1.7(e) 3 Aug 98  
9 (S//NF).

10  
11 b. (U) (b)(1) Sec 1.7(e) 30 Jun 97 (S).

12  
13 c. (U) (b)(1) Sec 1.7(e)  
14 (b)(1) Sec 1.7(e) (DRAFT) (S//NF).

15  
16 d. (U) (b)(1) Sec 1.7(e) 1 Jun 92  
17 (S//NF).

18  
19 e. (U) Joint Pub 2-01, Joint Intelligence Support to Military Operations,  
20 Appendix C, 7 Oct 04 (U).

21  
22 f. (U) (b)(1) Sec 1.7(e)  
23 (b)(1) Sec 1.7(e) 7 Mar 2006 (S//NF).

24  
25 1. (U) Situation. This appendix reviews general responsibilities and  
26 procedures for submitting (b)(1) Sec 1.7(e)  
27 (b)(1) Sec 1.7(e)

28  
29 a. (U) (b)(1) Sec 1.7(e) Refer to 8039 Annex B (Intelligence) (b)(1) Sec 1.7(e)  
30 (b)(1) Sec 1.7(e)

31  
32 b. (U) Friendly. Refer to Base Plan.

33  
34 c. (U) Assumptions. Refer to Base Plan.

35  
36 2. (U) Mission. Refer to Base Plan.

37  
38 3. (U) Execution. Refer to Annex B (Intelligence), para. 3.

39  
Classified by: Multiple Sources  
Reason: 1.4(a), (c), and (g)  
Declassify on: 26 February 2032

**SECRET**

SECRET

40 a. (U) Organization. USSTRATCOM/J2 (b)(1) Sec 1.7(e)  
41 management support to HQs staff elements per ref (f). USSTRATCOM JFCCs,  
42 components, and subordinate commands perform cyber operations (b)(1) Sec 1.7(e)  
43 (b)(1) Sec 1.7(e) for their organizations. JFCC ISR will closely  
44 collaborate with USSTRATCOM subordinate J2 (b)(1) Sec 1.7(e)  
45 (b)(1) Sec 1.7(e)  
46 (b)(1) Sec 1.7(e) Ultimately, reporting agencies will be responsible to the Command and its  
47 subordinates.

48  
49 b. (U) Concept of Operations. USSTRATCOM (b)(1) Sec 1.7(e)  
50 (b)(1) Sec 1.7(e) are assigned to USSTRATCOM,  
51 JFCCs, or other component organizations, CONOPS for the (b)(1) Sec 1.7(e)  
52 (b)(1) Sec 1.7(e) will be developed by the receiving  
53 organization and coordinated with USSTRATCOM/J2.

54  
55 (1) (U) Tasks. Not applicable.

56  
57 (2) (U) Requirements and Reporting. See refs (a) and (f) for the  
58 authorities, procedures, and formats for submitting (b)(1) Sec 1.7(e)  
59 (b)(1) Sec 1.7(e)

60  
61 (a) (C//REL) (b)(1) Sec 1.4(a)  
62 (b)(1) Sec 1.4(a)

63  
64  
65 (b) (U) (b)(1) Sec 1.7(e) See para. 3.b.(2)(a) above.

66  
67 (c) (U) External Tasking of (b)(1) Sec 1.7(e) Not  
68 applicable.

69  
70 (d) (U) Other (b)(1) Sec 1.7(e) Reporting Procedures/Formats. Not applicable.

71  
72 (e) (U) (b)(1) Sec 1.7(e)  
73 (b)(1) Sec 1.7(e)

74  
75  
76  
77  
78 c. (U) Coordination

79  
80 (1) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
81 (b)(1) Sec 1.4(a) in support of this CONPLAN.

82  
83 (2) (U) (b)(1) Sec 1.7(e) to USSTRATCOM  
84 provides (b)(1) Sec 1.7(e)  
85 coordination. The (b)(1) Sec 1.7(e) USSTRATCOM/J2 and other command

SECRET

~~SECRET~~

86 elements are kept fully aware of (b)(1) Sec 1.7(e)  
87 (b)(1) Sec 1.7(e) requirements.

88  
89 (3) (U) (b)(1) Sec 1.7(e)  
90 liaise with Commander, USSTRATCOM, component commands, and assigned  
91 units. (b)(1) Sec 1.7(e)  
92 (b)(1) Sec 1.7(e)

- 93  
94 4. (U) Administration and Logistics. See Annex B (Intelligence).  
95  
96 5. (U) Command and Control. See Annexes B (Intelligence) and J (Command  
97 and Control).  
98  
99 a. (U) Command Relationships. Not applicable.  
100  
101 b. (U) Communications. Not applicable.

102  
103  
104 Kevin P. Chilton  
105 General, USAF  
106 COMMANDER

~~SECRET~~

(INTENTIONALLY BLANK)

~~SECRET~~

B-5-4



**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
28 February 2008

APPENDIX 6 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039-07(U)  
(U) OPR: HQ USSTRATCOM/J2  
INTELLIGENCE SUPPORT TO INFORMATION OPERATIONS (IO) (U)

(U) References:

a. (U) Joint Pub 2-0, Joint Doctrine for Intelligence Support to Operations, 9 Mar 2000 (U).

b. (U) Joint Pub 2-01, Joint and National Intelligence Support to Military Operations, 7 Oct 2004 (U).

c. (U) Joint Pub 3-13, Joint Doctrine for Information Operations, 13 Feb 2006 (U).

d. (U) (b)(1) Sec 1.7(e) 13 Apr 2007 (U).

e. (U) Joint Pub 5-0, Doctrine for Planning Joint Operations, 26 Dec 2006 (U).

f. (U) Defense Intelligence Management Document, DI-2700-75-99, Analyst Information Requirements for Information Operations / Information Warfare, Feb 1999 (U).

1. (~~S//REL USA, AUS, GBR~~) Situation. This appendix specifies how information operations intelligence support will be conducted in support of USSTRATCOM CONPLAN 8039. See also Appendix 3 to Annex C (Information Operations) and Annex B (Intelligence).

a. (U) (b)(1) Sec 1.7(e) Refer to Annexes B (Intelligence) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

b. (U) Friendly

(1) (~~S//REL USA, AUS, GBR~~) Production Management. Production

Classified by: Multiple Sources  
Reason: 1.4(a), (c), and (g)  
Declassify on: 26 February 2032

**SECRET**

B-6-1

**SECRET**

40 management for this plan is organized using the IP processes and documented  
41 in the (b)(1) Sec 1.4(a) IO  
42 crosses the functional responsibility of several intelligence agencies and  
43 production centers often requiring direct coordination.

44 (2) (b)(1) Sec 1.4(a)  
45 (b)(1) Sec 1.4(a)  
46  
47

48  
49 (a) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
50 (b)(1) Sec 1.4(a)  
51

52  
53 (b) (S//REL USA, AUS, GBR TO USA, ACGU) (b)(1) Sec 1.4(a)  
54 (b)(1) Sec 1.4(a)  
55  
56

57  
58 (c) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
59 (b)(1) Sec 1.4(a)  
60 (b)(1) Sec 1.4(a) that assist a wide range of planning options.

61  
62 (d) (S//REL USA, AUS, GBR) USSTRATCOM and its JFCCs  
63 collaborate with the (b)(1) Sec 1.4(a)  
64 (b)(1) Sec 1.4(a) IO.

65  
66 (3) (S//REL USA, AUS, GBR) IO (b)(1) Sec 1.4(a) Information is  
67 (b)(1) Sec 1.4(a)  
68  
69 developed with:

70  
71 (a) (U) JCS - J2S: Coordination of Political-Military Assessments  
72 and compartmented requests for information (RFIs).

73  
74 (b) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
75 (b)(1) Sec 1.4(a)  
76  
77 level for support to 8039's intelligence requirements.

78  
79 (c) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
80 (b)(1) Sec 1.4(a)  
81  
82 the Headquarters building.

83  
84 (d) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) via an  
85 assigned LNO.

**SECRET**

86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131

(e) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(f) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

to enable combat commanders to develop operational courses of action. They serve operational

(b)(1) Sec 1.4(a)

databases, and detailed analysis.

(4) (U) Staff Coordination. Cyber intelligence requirements may require other support (e.g., collection and counter intelligence support). To facilitate this intelligence support, JIOWC coordinates with the following internal staff offices:

(a) (U) (b)(1) Sec 1.7(e)

(b) (U) (b)(1) Sec 1.7(e) support.

(c) (U) JIOWC Intelligence Operations assistance

(d) (U) (b)(1) Sec 1.7(e)

c. (U) Assumptions. Refer to the Base Plan and Annex B (Intelligence).

2. (U) Mission. Refer to the Base Plan.

3. (U) Execution

a. (~~S//REL USA, AUS, GBR~~) Operational Requirements. IO requires broad-based, dedicated intelligence support. (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

and access must be developed as early as possible. For example, (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

source of intelligence.

b. (~~S//REL USA, AUS, GBR~~) Information Requirements. (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

must be made. It is critical that (b)(1) Sec 1.4(a) of the

SECRET

132 (b)(1) Sec 1.4(a) kept  
133 current. Identifying requirements and initiating collection (b)(1) Sec 1.4(a)

134 (b)(1) Sec 1.4(a)  
135

136  
137 (1) (~~S//REL USA, AUS, GBR~~) Leadership. (b)(1) Sec 1.4(a) of  
138 key personnel, strategic communications, (b)(1) Sec 1.4(a)  
139 (b)(1) Sec 1.4(a) etc) will require updating.

140  
141 (2) (U) (b)(1) Sec 1.7(e)  
142 (b)(1) Sec 1.7(e)  
143

144  
145 (3) (U) (b)(1) Sec 1.7(e)  
146 (b)(1) Sec 1.7(e)  
147

148  
149 (4) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
150 (b)(1) Sec 1.4(a)  
151

152  
153 (5) (U) (b)(1) Sec 1.7(e)  
154 (b)(1) Sec 1.7(e) etc.  
155

156 (6) (U) Military and Civil (b)(1) Sec 1.7(e)  
157 (b)(1) Sec 1.7(e) for example.

158  
159 (7) (U) (b)(1) Sec 1.7(e)  
160 (b)(1) Sec 1.7(e) of the  
161 operation, for example.

162  
163 (8) (U) (b)(1) Sec 1.7(e)  
164 (b)(1) Sec 1.7(e)  
165  
166 validated prior to release.

167  
168 c. (U) Collection  
169

170 (1) (U) Collection Management. JIOWC will coordinate with respective  
171 J2 elements to ensure de-confliction of IO intelligence requirements.  
172

173 (2) (U) Supporting Systems  
174

175 (a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
176 requirements will focus on the aforementioned (b)(1) Sec 1.4(a)  
177 (b)(1) Sec 1.4(a)

178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223

(b) (U) (b)(1) Sec 1.7(e) supports all elements of IO. (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) of IO.

(c) (U) OSINT. Open Source Intelligence includes radio, television, speeches, newspapers, technical manuals, and the Internet. Along with public polling and survey data, such OSINT (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e)

(3) (~~S//REL USA, AUS, GBR~~) Capabilities Analysis. Access to (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) Additionally, intelligence to support cyberspace will require extensive (b)(1) Sec 1.4(a) analysts.

(4) (U) Processing, Production, Application, and Dissemination

(a) (U) Communication with Collection Management. Continuous assessment and analysis of intelligence collection is necessary in order to anticipate and/or react to the information situation as it develops.

(b) (U) Coordination. IO planners coordinate directly throughout the planning process and ensure that the appropriate J2 elements are included in planning at the appropriate phases.

(c) (U) Correlation. Information will be provided directly to the operator in a wide variety of formats. Products will be considered "draft" until reviewed and coordinated by the appropriate leadership.

(d) (U) Foreign Capability or Activity Assessment. N/A

(e) (U) (b)(1) Sec 1.7(e) to Annex B (Intelligence).

(f) (U) Database Management. Web-based tools and services, (b)(1) Sec 1.7(e)

(g) (U) (b)(1) Sec 1.7(e) N/A

(h) (U) C4 Network Analysis. USSTRATCOM plans, integrates and coordinates DOD GNO by directing GIG operations and defense, and identifies and advocates these desired characteristics and capabilities. USSTRATCOM

**SECRET**

224 integrates global C2 networks, identifies desired C2 capabilities, develops  
225 architectures and concepts, and manages doctrine development.  
226 USSTRATCOM's operations and C2 centers provide rapid integrated C2 for  
227 employing military capabilities.

228  
229 (i) (U) Capabilities Analysis. N/A

230  
231 4. (U) Sustaining Functions

232  
233 a. (~~S//REL USA, AUS, GBR~~) Automated data processing. Computer  
234 requirements must meet the accreditation requirements of the network. The

235 (b)(1) Sec 1.4(a)  
236  
237  
238  
239  
240

241  
242 (1) (U) (b)(1) Sec 1.7(e)

243  
244 (2) (U) (b)(1) Sec 1.7(e)

245  
246 (3) (U) (b)(1) Sec 1.7(e)

247  
248 (4) (U) (b)(1) Sec 1.7(e)

249 (b)(1) Sec 1.7(e)

250  
251 b. (U) Capabilities Analysis. Not used.

252  
253 c. (U) Communications. (b)(1) Sec 1.7(e)

254 (b)(1) Sec 1.7(e)  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269

~~SECRET~~

270

271 5. (U) Command and Control. Refer to Annex B (Intelligence).

272

273 |

274 |

275 Kevin P. Chilton

276 General, USAF

277 | COMMANDER

~~SECRET~~

B-6-7

**SECRET**

278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298

INTENTIONALLY BLANK

**SECRET**

B-6-8



# SECRET

221 (a) (U) OASD/PA provides overarching guidance and policy to  
222 combatant command PA personnel. This guidance will be disseminated by  
223 USSTRATCOM/PA and/or the supported/supporting GCC/PA.  
224

225 (b) (U) After the initial announcement of the execution of this plan,  
226 OASD/PA may delegate release authority to the supported commander. Once  
227 delegated this responsibility, the supported commander will determine if, when,  
228 and what release authority will be delegated to component/supporting  
229 commands and operational task forces.  
230

231 (c) (U) USSTRATCOM will lead the coordination of information  
232 among OASD/PA, JFCC NW/PA, JTF GNO/PA and the affected COCOM(s) as  
233 quickly and as often as required. USSTRATCOM will issue PA guidance as  
234 required.  
235

236 (d) (U) Detailed interaction and coordination among PA, IO, and  
237 DOD PA must occur throughout all phases of any operation.  
238

239 e. (U) Security Review. Although "information sharing" is key, PA offices at  
240 all levels must exercise "security at the source." OPSEC will be considered  
241 throughout all phases of the operation. The supported command PA function  
242 will conduct security and policy review when necessary.  
243

244 4. (U) Admin and Logistics. Refer to Base Plan.  
245

246 5. (U) Command and Control. Refer to Base Plan and Annex J (Command  
247 Relationships).  
248

249  
250 Kevin P. Chilton  
251 General, USAF  
252 Commander  
253

254 OFFICIAL:  
255

256  
257 JILL H. VOTAW  
258 CAPT, USN  
259 Chief, Public Affairs  
260  
261

# SECRET

# ~~SECRET~~

175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220

(a) (U) Ensure subordinate units receive and comply with the PA policy and guidance in this Annex, and any other specified OASD/PA-approved PAG.

(b) (U) Propose information that can be used for a detailed PA communication plan, or Proposed Public Affairs Guidance (PPAG).

(c) (U) Coordinate any planned PA programs and activities related to this plan with USSTRATCOM/PA.

(d) (U) Develop local PA annexes to supporting plans assigning responsibilities and providing command-specific guidance (public information, internal information, and community relations) necessary to successfully implement this plan. As appropriate, coordinate PA annexes of supporting plans with logistics, communications and operations planners, and USSTRATCOM/PA.

(e) (U) Be prepared to exercise release authority delegated to Component Commanders or Task Force Commanders (TFC).

(f) (U) Provide Component Commanders and TFCs advice and counsel on PA matters concerning USSTRATCOM operations, as required, and immediately inform USSTRATCOM/PA of any incident or action resulting from communications that are likely to require action at the USSTRATCOM; Service; Joint Staff or OASD level; be of immediate news interest; or cause unfavorable public reaction or publicity.

## d. (U) Coordinating Instructions

(1) (U) Release Authority. Release authority will be delegated to the lowest level possible consistent with published PA guidance.

(2) (U) Reporting Requirements. All supporting PA functions will provide a daily SITREP, by 1700 ZULU, to USSTRATCOM/PA, via NIPR email if possible. The SITREP will include: electronic copies or internet links of articles published in the preceding 24 hours; planned press releases; a summary of completed PA actions and future media engagements; a list of PA personnel deployed; and any new messages or talking points. USSTRATCOM will publish a consolidated SITREP each day.

(3) (U) There will be no releases, statements, responses to media inquiries or other public announcements by USSTRATCOM or assigned forces concerning this plan without authorization from OASD/PA. The general conduct and control of PA activities will be as follows:

~~SECRET~~

# SECRET

129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174

(1) (U) PA will:

(a) (U) Be involved in all appropriate planning boards and groups to include Information Operations Working Groups (IOWG), Operational Planning Groups and Long Range Planning Elements, etc.

(b) (U) Plan for specific contingencies and formulate tailored courses of action for each Phase of operations to affect regional and international opinion.

(c) (U) Counter enemy propaganda with the truth. Actively use truthful, fact-based, accurate and timely public information products to respond to enemy threats, deception and lies.

(d) (U) Ensure all personnel required to interact with media and the community are well-versed on the PA guidance, media guidelines, and prepared to assist media members as necessary.

(e) (U) As news releases and statements are issued to the media, they should also be disseminated to the internal audience via SKIWEB, STRATWEB, and other available resources.

(2) (U) CDRUSSTRATCOM will: Assign high priority to PA programs and direct commanders to assign dedicated assets and support a PA program consistent with OPSEC, INFOSEC, PAG, regulations and policies.

(3) (U) USSTRATCOM/PA will:

(a) (U) Provide CDRUSSTRATCOM and his staff advice and counsel on PA matters concerning operations as required. Develop PA policy, guidance and plans as required.

(b) (U) Maintain liaison with OASD/PA, JFCC NW/PA, JTF\_GNO/PA, and GCC/PAs on PA policy matters.

(c) (U) Coordinate PA activities with IO and SC to synchronize themes and messages.

(d) (U) Ensure rapid communication of PAG to component and task force PA offices.

(4) (U) Geographic Combatant Command PA (GCC/PA) will: Provide regular feedback on significant PA activity within the area of responsibility/ area of interest to OASD/PA, CJCS/PA and USSTRATCOM/PA.

(5) (U) USSTRATCOM Component Command /Task Force PA Offices will:

# SECRET

# SECRET

83 used as a military deception capability or to provide disinformation to internal  
84 or external audiences.

85

86 2. (U) Mission. Refer to Base Plan.

87

88 3. (U) Execution

89

90 a. (U) Concept of Operations. The supported command for execution will  
91 lead the efforts to develop, coordinate and synchronize a comprehensive PA  
92 program with the supporting PA functions and OASD/PA, which is aligned with  
93 and directly supports USG communication objectives. As a supporting  
94 command, USSTRATCOM retains responsibility for providing coordinated JFCC  
95 NW and JTF GNO PA products (in addition to other USTRATCOM components  
96 as applicable) to the supported command PA function. Regardless, the intent  
97 is to provide truthful information of sufficient breadth and timeliness which  
98 supports the efforts to educate the audience with the cyberspace domain and  
99 its impact on military operations.

100

101 b. (U) Themes and Messages. The following overarching themes and  
102 messages are contained in NSPD 38.

103

104 (1) (U) The US is committed to ensuring the free and secure flow of  
105 information through cyberspace. Global economic growth and security depend  
106 upon the networks and systems that constitute cyberspace. Maintaining  
107 freedom of action in cyberspace in the 21<sup>st</sup> Century is as inherent to US  
108 interest as freedom of the seas became in the 19<sup>th</sup> Century and access to air  
109 and space in the 20<sup>th</sup> Century.

110

111 (2) (U) We will continue to lead international and domestic efforts to  
112 ensure the security of global information infrastructures upon which  
113 cyberspace depends.

114

115 (3) (U) The US reserves the right to respond to attacks in and through  
116 cyberspace by nations, terrorist groups, or other adversaries in a manner it  
117 deems appropriate.

118

119 (4) (U) We will maintain the capabilities to operate in the cyberspace  
120 domain to deter, deny, or defeat any adversary that seeks to harm US national  
121 and economic security.

122

123 (5) (U) We will ensure that our actions in this domain are undertaken in  
124 a manner that is lawful and protects our Constitutional liberties.

125

126 c. (U) Tasks. Consistent with current OASD/PA guidance, and within the  
127 constraints of Operations Security (OPSEC), Information Security (INFOSEC),  
128 safety and privacy of US military personnel, their families and DOD civilians;

SECRET

**SECRET**

38 k. (U) DOD Instruction 5410.19, Public Affairs Community Relations Policy  
39 Implementation, 13 November 2001

40  
41 1. (U) Situation

42  
43 a. (U) General

44  
45 (1) (U) This annex assigns responsibilities and provides overarching  
46 guidance for military Public Affairs (PA) activities in support of  
47 CDRUSSTRATCOM CONPLAN 8039-07(S) for combatant and supporting  
48 commands.

49  
50 (2) (U) The preeminent factor in PA support of this strategic concept  
51 involves coordinating and communicating DOD efforts in broad themes and  
52 public affairs strategies by establishing a common context in the cyberspace  
53 domain for military areas of operation and developing a deeper understanding  
54 of this domain and its impact on warfighting. In support of this plan, PA  
55 efforts must be well-synchronized with other USG and DOD communication  
56 strategies. This requires a comprehensive PA plan that extends from OASD/PA  
57 to USSTRATCOM, its components, and integrated with Geographic Combatant  
58 Commands (GCC) (b)(1) Sec 1.7(e)

59 (b)(1) Sec 1.7(e)

60  
61 b. (U) (b)(1) Sec 1.7(e) Refer to Base Plan.

62  
63 c. (U) Friendly. Refer to Base Plan.

64  
65 d. (U) Assumptions. Refer to Base Plan.

66  
67 e. (U) Policy. PA is a function of command and consists of public  
68 information, internal (or command) information, and community relations  
69 activities designed to educate and inform external and internal publics and  
70 stakeholders. Public Affairs activities are conducted in accordance with  
71 existing DOD directives and policy, the DOD Principles of Information, and  
72 current Office of Assistant Secretary of Defense for Public Affairs (OASD/PA)  
73 guidance. Other policy considerations follow:

74  
75 (1) (U) PA activities are complementary to, yet distinct from, Information  
76 Operations (IO). PA activities contribute to IO by providing truthful, fact-based,  
77 accurate and timely information, using approved OASD public affairs guidance  
78 (PAG), to keep the public informed about the military's missions and operations  
79 in support of military objectives, countering enemy propaganda, dissuading  
80 and deterring enemy actions, and maintaining the trust and confidence of the  
81 US population, our friends and allies. By law, and by doctrine, PA activities  
82 are prohibited from intentionally deceiving the public. PA activities will not be

**SECRET**

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AFB, NE 68113-6500  
28 February 2008

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37

ANNEX F TO CDRUSSTRATCOM CONPLAN 8039 (U)

(U) OPR: USSTRATCOM J020

PUBLIC AFFAIRS (U)

(U) References: Refer to Base Plan.

a. (U) JP 3-61, Doctrine for Public Affairs in Joint Operations, 14 May 1997

b. (U) DOD Directive 5122.5, Assistant Secretary of Defense for Public Affairs, 27 Sep 2000

c. (U) DOD Directive 5200.1, DOD Information Security Program, 13 December 1996

d. (U) DOD Directive 5230.9, Clearance of DOD Information for Public Release (Change 1), 15 July 1999

e. (U) DOD Instruction 5230.29, Security and Policy Review of DOD Information for Public Release, 6 August 1999

f. (U) DOD Directive 5400.13, Joint Public Affairs Operations, 9 January 1996

g. (U) DOD Instruction 5400.14, Procedures for Joint Public Affairs Operations, 22 January 1996

h. (U) DOD Instruction 5405.3, Development of Proposed Public Affairs Guidance, 5 April 1991

i. (U) DOD Instruction 5410.15, DOD Public Affairs Assistance to Non-Government, Non-Entertainment-Oriented Print and Electronic Media, 28 March 1989

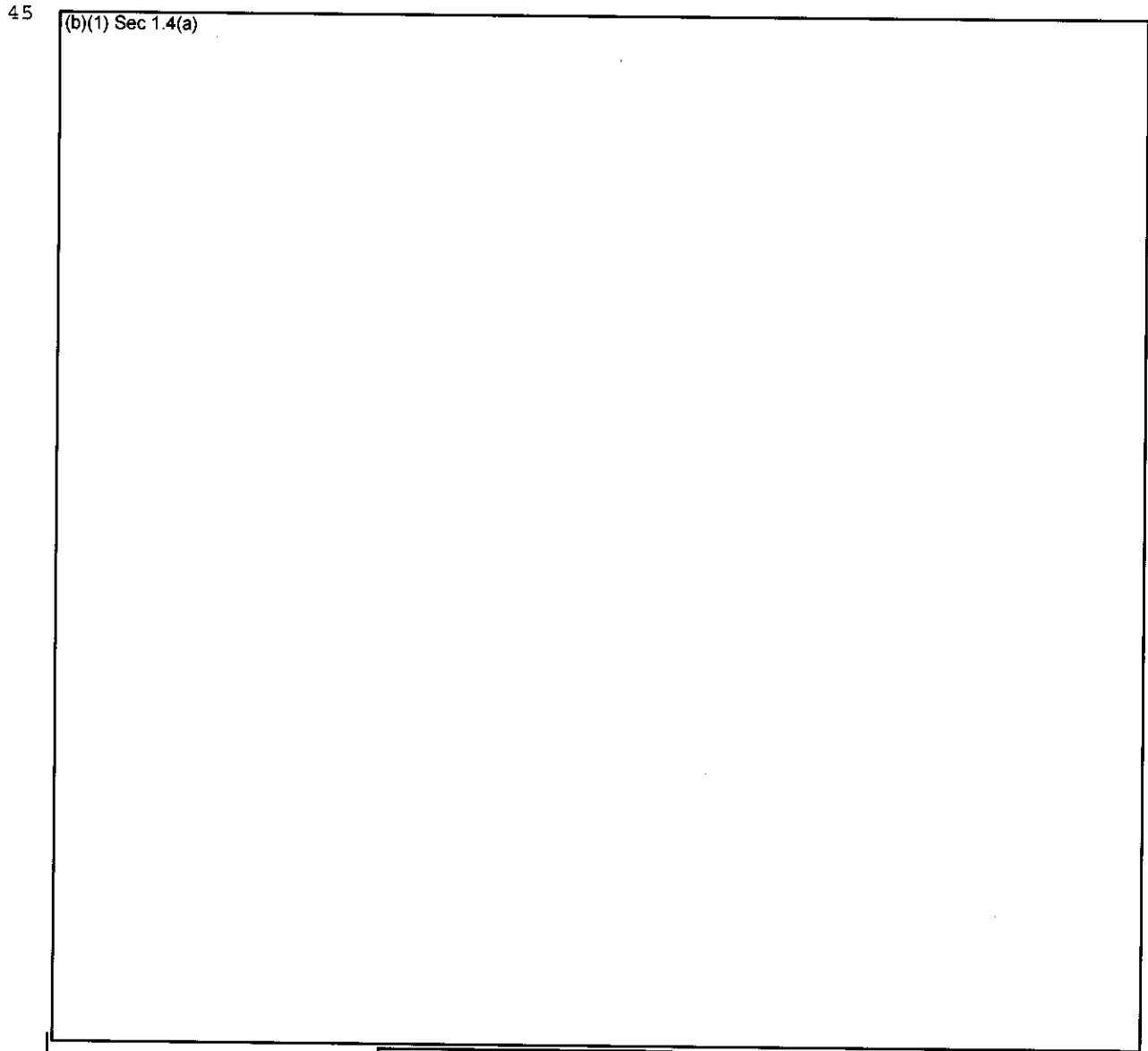
j. (U) DOD Directive 5410.18, Community Relations Policy, 20 November 2001

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (c), and (g)~~  
~~Declassify on: 27 February 2033~~

**SECRET**

**SECRET**

42 (4) (U) Other USSTRATCOM components will review and provide  
43 CONPLAN 8039 (b)(1) Sec 1.4(a) additions and  
44 deletions, to USSTRATCOM J534.



46 Figure C-20-1, (b)(1) Sec 1.4(a) (S//REL USA, AUS, GBR)

47

48 4. (U) Administration and Logistics. Refer to Base Plan.

49

50 5. (U) Command and Control. Refer to Base Plan.

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (c), and (g)~~  
~~Declassify on: 27 February 2033~~

**SECRET**

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE NE 68133-6500  
27 February 2008

APPENDIX 20 TO ANNEX C TO CDR USSTRATCOM CONPLAN 8039 (U)

(U) OPR: JFCC NW J52

(b)(1) Sec 1.7(e) (U)

(U) References: Refer to Base Plan and Annex C (Operations).

1. (U) Situation. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

a. (~~S//REL USA, AUS, GBR~~) Concept of Operation. The (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

of the Base Plan.

b. (U) Tasks

(1) (U) HQ USSTRATCOM J534 will maintain the CONPLAN 8039 (b)(1) Sec 1.7(e) and receive inputs from USSTRATCOM components during CONPLAN 8039 periodic reviews.

(2) (~~S//REL USA, AUS, GBR~~) JTF\_GNO will review and provide CONPLAN 8039 (b)(1) Sec 1.4(a) to include recommended additions and deletions, to USSTRATCOM J534 for (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(3) (~~S//REL USA, AUS, GBR~~) JFCC NW will review and provide CONPLAN 8039 (b)(1) Sec 1.4(a) additions and deletions, to USSTRATCOM J534 for (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)



332 operational or strategic level. (b)(1) Sec 1.7(e)  
333 (b)(1) Sec 1.7(e)  
334  
335

336 (6) (U) (b)(1) Sec 1.7(e)  
337 (b)(1) Sec 1.7(e)  
338  
339  
340  
341  
342

343 (7) (U) Operational Effects: Desired operational-level outcomes  
344 necessary to achieve a phase objective. Operational effects incorporate all  
345 elements of national power available to the theater commander.  
346

347 (8) (U) (b)(1) Sec 1.7(e)  
348 (b)(1) Sec 1.7(e)  
349  
350

351 (b)(1) Sec 1.7(e) systems for a specific purpose.  
352

353 (9) (U) Political, Military, Economic, Social, Infrastructure, and  
354 Information (PMESII): Construct for defining systems behaviors.  
355

356 (10) (U) (b)(1) Sec 1.7(e)  
357 (b)(1) Sec 1.7(e)  
358  
359

360 throughout the campaign.  
361

362 f. (U) Tasks. Refer to Base Plan.  
363

364 g. (U) Coordinating Instructions. Refer to Base Plan.  
365

366 4. (U) Administration and Logistics. Refer to Base Plan.  
367

368 5. (U) Command and Control. Refer to Base Plan.

SECRET

286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331

(b)(1) Sec 1.4(a)

circumstances.

d. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) Commanders at all levels will ensure that (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) USSTRATCOM will integrate and coordinate DOD Components plans and address synchronization, advocacy, and allocation issues that arise.

e. (U) Definitions

(1) (U) Campaign effects: Desired theater-level outcomes or conditions that allow CDR UNC/CFC to achieve the operational objectives.

(2) (U) Effect: The physical, functional, or psychological outcome, event or consequence that results from a specific action or actions that produces desired changes in enemy actions, reactions, or inability to act.

(3) (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) provides a conceptual alternative to traditional attrition and maneuver warfare.

(b)(1) Sec 1.7(e)

(4) (U) Indicator: criteria that we are going to measure. Indicators may

(b)(1) Sec 1.7(e)

(5) (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

# SECRET

240 (1) (U) Reassess the adversary utilizing the (b)(1) Sec 1.7(e) and  
241 threat analysis to determine the new (if any) cyberspace operations threat  
242 posed by that adversary.  
243

244 (2) (U) Reassess the (b)(1) Sec 1.7(e) and determine if the  
245 actions applied cause a significant change in capability or intent of the actor.  
246

247 (3) (U) Determine if any (b)(1) Sec 1.7(e) were met.  
248

249 (4) (U) Assess resources to ensure current resources are  
250 adequate and sufficient. If additional resources or capabilities are required,  
251 USSTRATCOM, JCS, and OSD must re-enter the DOD PPBS cycle to address  
252 near and long term needs and to acquire, as quickly as possible, capabilities  
253 that address immediate needs.  
254

255 (5) (U) Determine unintentional and undesired effects of  
256 actions applied. Ensure other DOD Components and USG agencies are aware  
257 of actions, as effects in cyberspace (with few exceptions) are trans-regional.  
258

259 b. (U) If the applied tasks were not successful in achieving  
260 the desired effect:  
261

262 (1) (U) Reassess the actor utilizing the (b)(1) Sec 1.7(e) and  
263 threat analysis to determine the new (if any) cyberspace operations threat that  
264 the adversary actor poses remains valid.  
265

266 (2) (U) Evaluate the (b)(1) Sec 1.7(e)  
267

268 (3) (U) Determine if other associated effects were  
269 met.  
270

271 (4) (U) Assess current resources to ensure adequacy  
272 and sufficiency. If additional resources or capabilities are required,  
273 USSTRATCOM, JCS, and OSD must re-enter the DOD PPBS cycle to address  
274 near and long term needs and to acquire, as quickly as possible, capabilities  
275 that address immediate needs.  
276

277 (5)(U) Determine if any unintentional and or  
278 undesired effects occurred. Ensure other DOD Components and USG agencies  
279 are aware of actions, as effects in cyberspace (with few exceptions) are trans-  
280 regional.

281 c. (~~S//REL USA, AUS, GBR~~) Interagency Efforts. Refer to Annex V  
282 (Interagency). USSTRATCOM, through OSD, JS, and in coordination with the  
283 applicable Combatant Commands' (b)(1) Sec 1.4(a) will engage the interagency to  
284 develop a common situational awareness of USG, (b)(1) Sec 1.4(a) and  
285 (b)(1) Sec 1.4(a) threats in cyberspace. (b)(1) Sec 1.4(a)

# SECRET

C-19-8

SECRET

196 processes, the USSTRATCOM staff develops a (b)(1) Sec 1.4(a) across  
197 (b)(1) Sec 1.4(a)  
198  
199

200 (c) (U) (b)(1) Sec 1.7(e) Assessment  
201 Guidance.

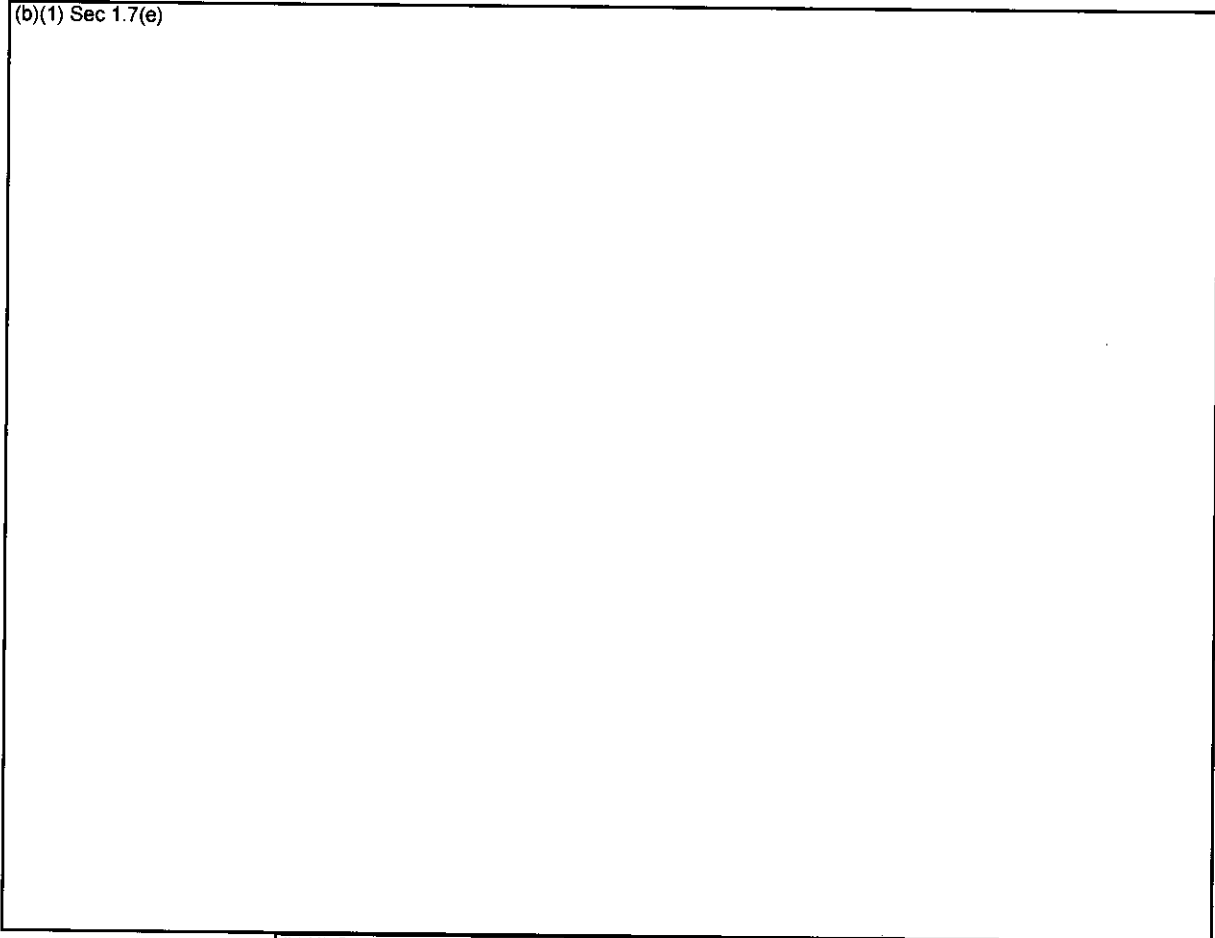
202  
203 1 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) Using available  
204 assessments and analysis, the (b)(1) Sec 1.4(a)  
205 (b)(1) Sec 1.4(a)  
206 operations in and through cyberspace. This may (b)(1) Sec 1.4(a)  
207 to re-align with new combatant commander's priorities.

208  
209 2 (U) Assessing Effectiveness. Following the execution of  
210 cyberspace operations applied tasks; commanders responsible for the  
211 execution of those applied tasks assess the performance of tasks and report  
212 findings to the (b)(1) Sec 1.7(e)  
213

214 3 (U) Assessing (b)(1) Sec 1.7(e) defined in para  
215 3e(5)). USSTRATCOM HQ staff and applicable components assess (b)(1) Sec 1.7(e) for  
216 individual tasks conducted during the course of operations. When performing  
217 this assessment, answer the following questions: Are we doing things right?  
218 Were the tasks performed correctly? Insights into this aspect of task execution  
219 inform advocacy and military decision-making processes that support the  
220 cyberspace operations campaign cycle. The assessment of (b)(1) Sec 1.7(e) for newly  
221 integrated capabilities across the DOTMLPF informs the advocacy process by  
222 (b)(1) Sec 1.7(e) operational needs in terms of support  
223 and sufficiency. USSTRATCOM will assign an Office of Primary Responsibility  
224 (OPR) to each applied task. The OPR (b)(1) Sec 1.7(e)  
225 (b)(1) Sec 1.7(e) for each applied task.

226  
227 4 (U) Assessing (b)(1) Sec 1.7(e) defined in para  
228 3e(4)). USSTRATCOM and Components must also assess the (b)(1) Sec 1.7(e)  
229 (b)(1) Sec 1.7(e)  
230 (b)(1) Sec 1.7(e) will answer the questions: Are we doing the  
231 right things? Did the applied task have the desired effect on the threat?  
232 USSTRATCOM will assign an OPR to each applied task. The OPR (b)(1) Sec 1.7(e)  
233 (b)(1) Sec 1.7(e)  
234  
235

236  
237 a. (U) If the applied tasks were successful in achieving the  
238 desired effect:  
239



176 Figure C-19-2, (b)(1) Sec 1.7(e) briefing, May 2006) (U)

177  
178 (3) (U) (b)(1) Sec 1.7(e)

179  
180 (a) (U) (b)(1) Sec 1.7(e) The linkage above provides a baseline starting point  
181 to develop (b)(1) Sec 1.7(e)  
182 (b)(1) Sec 1.7(e)  
183 operational level applied tasks.

184  
185 (b) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) Once specific  
186 (b)(1) Sec 1.4(a)

187  
188 (b)(1) Sec 1.4(a) The overall  
189 criteria for the actual prioritization (b)(1) Sec 1.4(a)  
190 (b)(1) Sec 1.4(a)  
191  
192  
193  
194  
195

**SECRET**

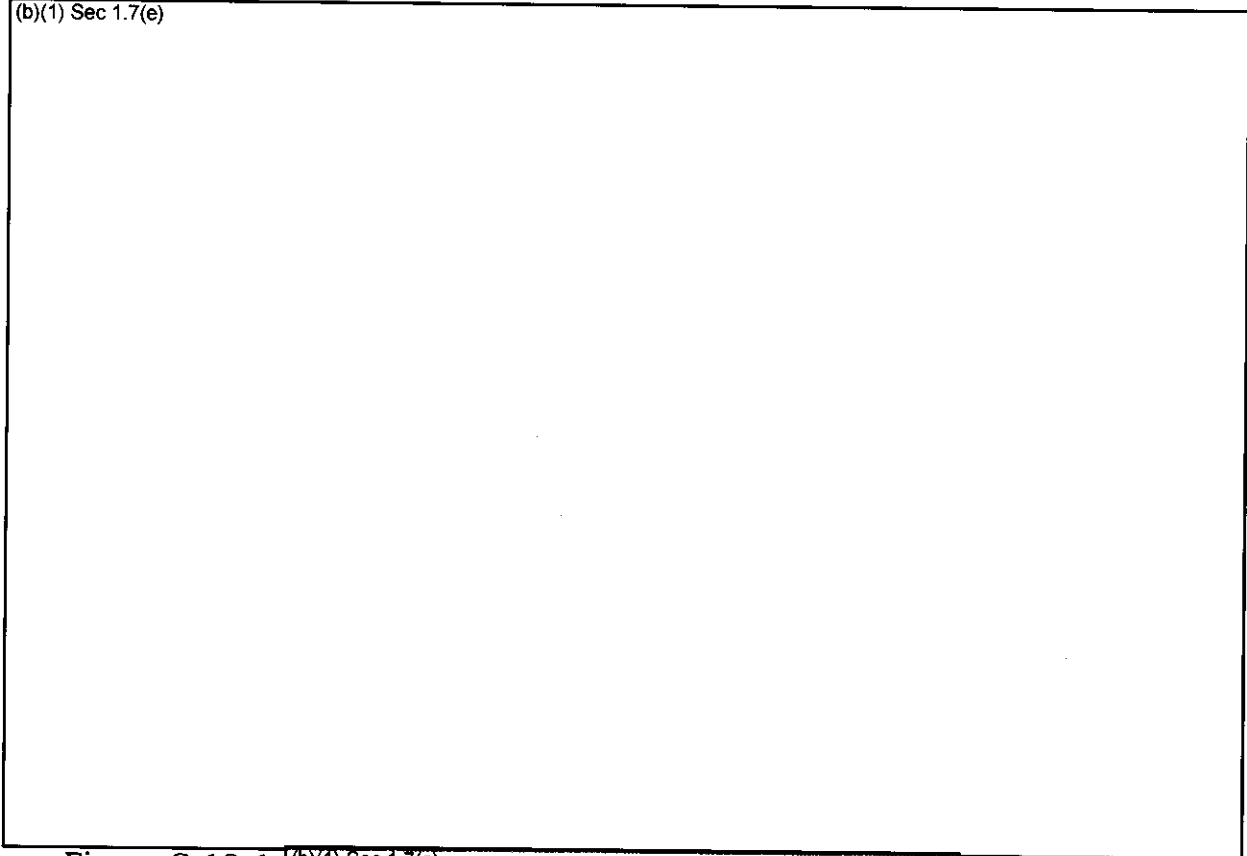
139 (b) (U) The USSTRATCOM staff and components analyze the mission  
140 using all tools available- Operational Net Assessment (ONA, defined in para  
141 3e(8)), CIE COA analysis, Virtual Information Environment (VIE), etc to  
142 understand the operational environment and determine what Political, Military,  
143 Economic, Social, Infrastructure, and Information (PMESII, defined in para  
144 3e(10)) system behaviors and /or capabilities - (b)(1) Sec 1.7(e)  
145 (b)(1) Sec 1.7(e) COCOM theater objectives.  
146

147 (c) (U) Based on CDRUSSTRATCOM's verification of the task to  
148 objectives and the analysis of the adversary and the operational environment  
149 provided by the staff and components, the commander's intent is issued to all  
150 components and supporting agencies. This normally includes his vision of  
151 what needs to be done (purpose), a broad concept for how CDRUSSTRATCOM  
152 intends to accomplish the objectives (method) and key measures for  
153 determining success (end state). CDRUSSTRATCOM provides planning  
154 guidance to focus staff and component development of COAs to accomplish his  
155 vision/end state for (b)(1) Sec 1.7(e)  
156 CONPLAN 8039). COAs within (b)(1) Sec 1.7(e)  
157 (b)(1) Sec 1.7(e) will fuse and synchronize the appropriate DIME and/or PMESII  
158 actions, in time and space, against those decisive points within the operational  
159 environment which most directly produce the effects that will achieve his  
160 stated objectives. The goal is unity of effort or harmonization of all elements of  
161 DIME/PMESII toward a common goal.  
162

163 (d) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
164 which produce decision points (b)(1) Sec 1.4(a)  
165 (b)(1) Sec 1.4(a)  
166 based upon the commander's guidance and intent. Refer to Base Plan for  
167 CONPLAN 8039 (b)(1) Sec 1.4(a)  
168

169 (e) (U) USSTRATCOM integration and collaboration mechanisms will  
170 be used to develop (b)(1) Sec 1.7(e)  
171 (b)(1) Sec 1.7(e) which is the primary means to provide operational level assessment.  
172 All appropriate DOD Components and USG Agencies will be invited to  
173 participate. (b)(1) Sec 1.7(e) (See  
174 Figure C-19-2 below).  
175

(b)(1) Sec 1.7(e)



118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138

Figure C-19-1, (b)(1) Sec 1.7(e) May 2006) (U)

(1) (U) Evaluate and Prioritize Threat. (See (b)(1) Sec 1.7(e) for a detailed discussion of the (b)(1) Sec 1.7(e).

(2) (U) Tailored Planning

(a) (U) The tailored planning process uses an (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) Through an analysis of the national strategic objectives, utilizing the products from the (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) USSTRATCOM develops (b)(1) Sec 1.7(e)

(CONPLAN 8039, reference chart with (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

**SECRET**

83 (b)(1) Sec 1.7(e)

84 CONPLAN 8039 Base Plan.

85  
86 4 (U) Emphasizes unity of effort through a strengthening of  
87 interagency operations by:

88  
89 a. (U) Supporting improvements in strategy development  
90 and planning within DOD and with interagency partners to shift emphasis  
91 from DOD-centric approaches toward USG interagency and coalition/allied  
92 solutions.

93  
94 b. (U) Developing stronger links between planners in the  
95 OSD, the Joint Staff, Combatant Commands, Services and the IC.

96  
97 c. (U) Facilitating communication by developing shared  
98 perspectives and a better understanding of each agency's roles, missions, and  
99 capabilities.

100  
101 d. (U) Improving the effectiveness of operations in and  
102 through cyberspace through the accomplishment of objectives and promoting  
103 efficiency throughout the operational mission area by effectively allocating,  
104 integrating, and using limited resources.

105  
106 (c) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) established  
107 for this appendix (b)(1) Sec 1.4(a)  
108 (b)(1) Sec 1.4(a) and as referenced in the CONPLAN 8039 base  
109 plan (para 3.a.(3)).

110  
111 b. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
112 This appendix provides a framework for continuous and sustained efforts  
113 throughout DOD (b)(1) Sec 1.4(a)  
114 (b)(1) Sec 1.4(a)  
115 (b)(1) Sec 1.4(a) in an operational  
116 environment).



**SECRET**

40 (3) (U) (b)(1) Sec 1.7(e) Refer to Base Plan and Annex A (Task  
41 Organization).

42 (4) (U) (b)(1) Sec 1.7(e) Refer to Base Plan and Annex B  
43 (Intelligence) (b)(1) Sec 1.7(e)

45 (5) (U) Friendly Capabilities. Refer to Base Plan and Annex A (Task  
46 Organization).

48 (6) (U) Assumptions. Refer to Base Plan and Annex C (Operations).

50 (7) (U) Legal Considerations. Refer to Base Plan and Annex C  
51 (Operations).

53 2. (U) Mission. Refer to Base Plan.

55 3. (U) Execution

57 a. (U) Concept of Operations

59 (1) (U) Commander's Intent

61 (a) (~~S//REL USA, AUS, GBR~~) Purpose. The purpose of CONPLAN  
62 8039 (b)(1) Sec 1.4(a)

63 (b)(1) Sec 1.4(a)

64 The purpose of this appendix is to set the framework for integration and  
65 synchronization of USSTRATCOM plans in support of operations in and  
66 through cyberspace, and define activities and metrics to assess their  
67 effectiveness. (b)(1) Sec 1.4(a)

68 (b)(1) Sec 1.4(a)

72 (b) (U) Method. This appendix uses a strategic framework that:

74 1 (U) Includes a process for the development of a (b)(1) Sec 1.7(e)  
75 (b)(1) Sec 1.7(e) for CONPLAN 8039 is shown at Appendix 20 to Annex C.

77 2 (U) Includes an (b)(1) Sec 1.7(e) to describe the overall  
78 (b)(1) Sec 1.7(e)

81 3 (U) Includes logical lines of operation in which DOD will focus  
82 (b)(1) Sec 1.7(e)

SECRET

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE NE 68133-6500  
28 February 2008

APPENDIX 19 TO ANNEX C TO USSTRATCOM CONPLAN 8039 (U)

(U) OPR: JFCC NW/J52

(b)(1) Sec 1.7(e) GUIDANCE (U)

References: Refer to Base Plan.

a. (U) Commander's Handbook for an (b)(1) Sec 1.7(e) to Joint Operations, 24 Feb 06

1. (~~S//REL USA, AUS, GBR~~) Situation. Since the advent of the Information Age, the US, at all levels of government and society, has become increasingly dependent upon the world-wide network of software, computers, and telecommunications infrastructure as the foundation of our national economy.

DOD (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

a. (U) General

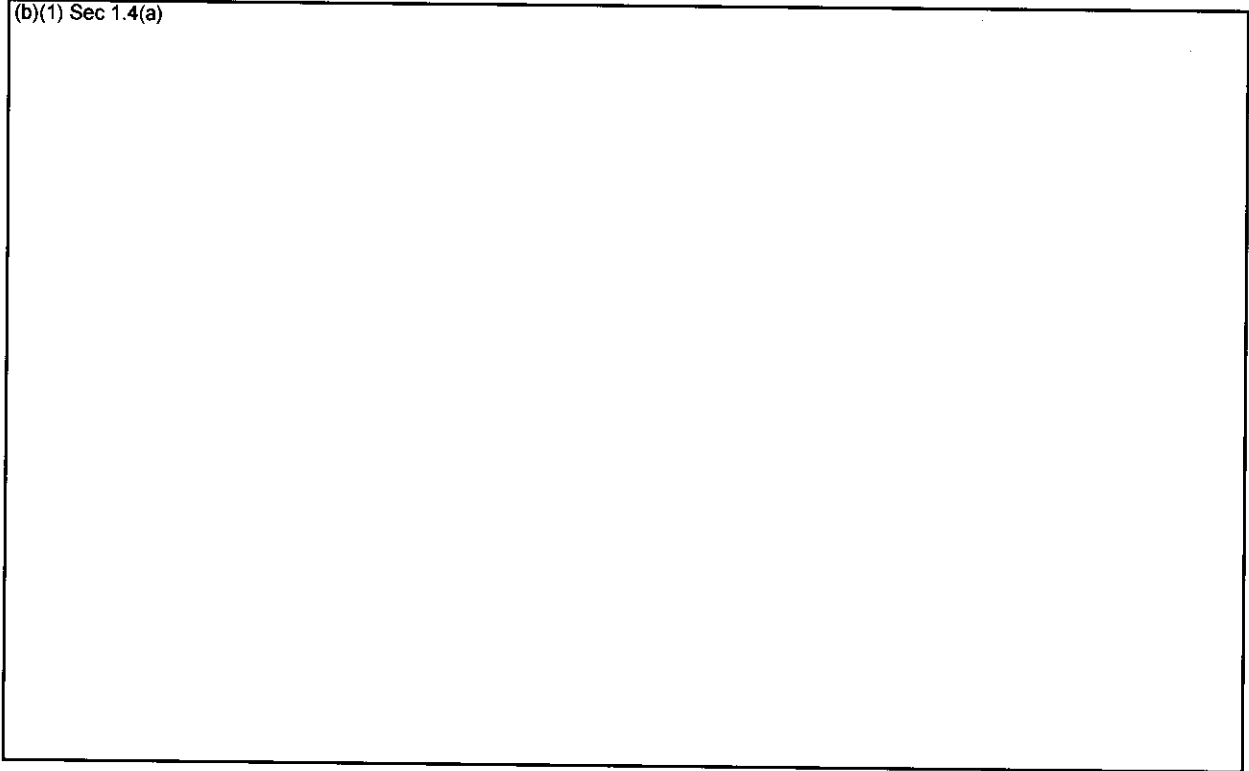
(1) (~~S//REL USA, AUS, GBR~~) Function. This appendix describes plans and functions to integrate and synchronize STRATCOM's (b)(1) Sec 1.4(a) within the DOD GIG and operations in and through cyberspace in support of (b)(1) Sec 1.4(a) USSTRATCOM command goal. This appendix also expands upon the (b)(1) Sec 1.4(a) described in the CONPLAN 8039 Plan Summary (para 1.b(1)), Base Plan, and Annex C to (b)(1) Sec 1.4(a). This appendix describes the strategic framework within the (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) cyberspace operations.

(2) (U) Area of Concern. Refer to Base Plan.

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (c), and (g)~~  
~~Declassify on: 27 February 2033~~

**SECRET**

(b)(1) Sec 1.4(a)



207  
208

Figure C-18-3 - (b)(1) Sec 1.4(a) (S//REL USA, AUS, GBR)

**SECRET**

C-18-8

**SECRET**

182 (3) (~~S//REL USA, AUS, GBR~~) ICW JFCC GSI (b)(1) Sec 1.4(a)

183 (b)(1) Sec 1.4(a)

185 (4) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

187 (b)(1) Sec 1.4(a)

188 (5) (~~S//REL USA, AUS, GBR~~) Identify COA support requirements

190 (b)(1) Sec 1.4(a)

192 (6) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

193 (b)(1) Sec 1.4(a) if identified as supported commander.

194 (7) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

196 JFCC GSI a post mission analysis feedback.

197 (8) (~~S//REL USA, AUS, GBR~~) Request assistance in organizing, training  
198 and otherwise preparing (b)(1) Sec 1.4(a) from JFCC GSI, if required.

200 (9) (~~S//REL USA, AUS, GBR~~) Support JFCC GSI through the (b)(1) Sec 1.4(a)

202 (b)(1) Sec 1.4(a)

204 c. Figure C-18-2 below is a graphical depiction of (b)(1) Sec 1.4(a)

206

SECRET

137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181

(3) ~~(S//REL USA, AUS, GBR)~~ Prepare and maintain plans in support of  
(b)(1) Sec 1.4(a)

(4) ~~(S//REL USA, AUS, GBR)~~ Recommend (b)(1) Sec 1.4(a) when appropriate.

(5) ~~(S//REL USA, AUS, GBR)~~ Establish (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(6) ~~(S//REL USA, AUS, GBR)~~ Coordinate and lead the (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) development.

(7) ~~(S//REL USA, AUS, GBR)~~ Provide support to (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) as required or directed.

(8) ~~(S//REL USA, AUS, GBR)~~ In preparation for follow-on operations, monitor situations generated intelligence, follow-on operations possibilities, additional coordination requirements, (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(U) (9) ~~(S//REL USA, AUS, GBR)~~ Ensure all open action items are evaluated for closure.

(10) ~~(S//REL USA, AUS, GBR)~~ (b)(1) Sec 1.4(a) conduct a post-mission analysis.

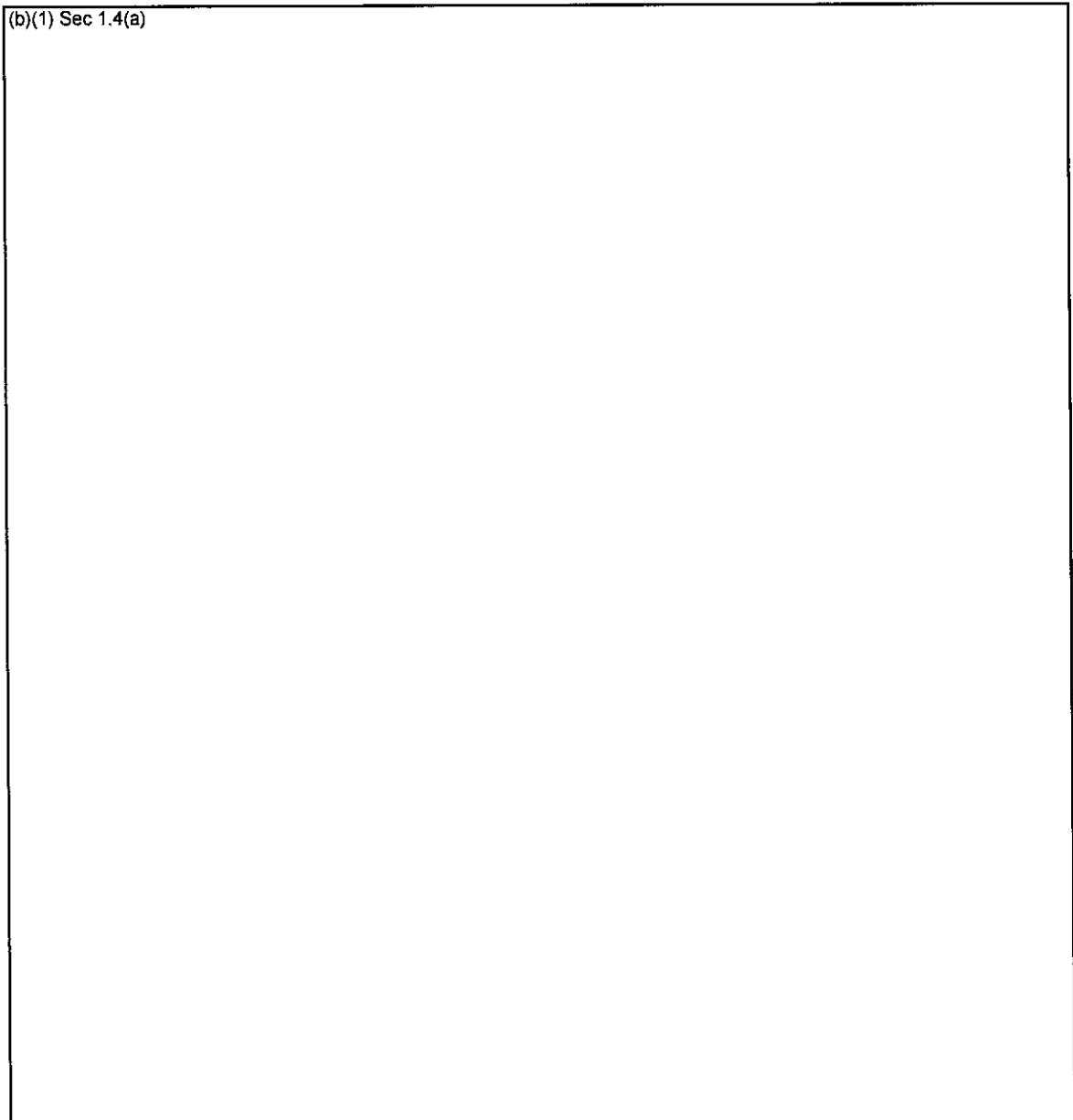
(11) ~~(S//REL USA, AUS, GBR)~~ Assist in organizing, training and otherwise preparing (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

b. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

(1) ~~(S//REL USA, AUS, GBR)~~ Using existing infrastructures (i.e. CAT, Crisis Action Center [CAC], Command Center, Operations Center, Joint Operations Center [JOC], JIOC), (b)(1) Sec 1.4(a) The GCC determines the appropriate command and structure arrangements for respective (b)(1) Sec 1.4(a)

(2) ~~(S//REL USA, AUS, GBR)~~ (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)



124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136

Figure C-18-2 - (b)(1) Sec 1.4(a) (S//REL USA, AUS, GBR)

3. (U) (b)(1) Sec 1.7(e) Responsibilities and Requirements.

a. (U) USSTRATCOM.

(1) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) operations under this plan, as required.

(2) (~~S//REL USA, AUS, GBR~~) Monitor through JFCC GSI (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

**SECRET**

104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123

(2) (~~S//REL USA, AUS, GBR~~) CDRUSSTRATCOM will review the  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) USSTRATCOM operational recommendation.

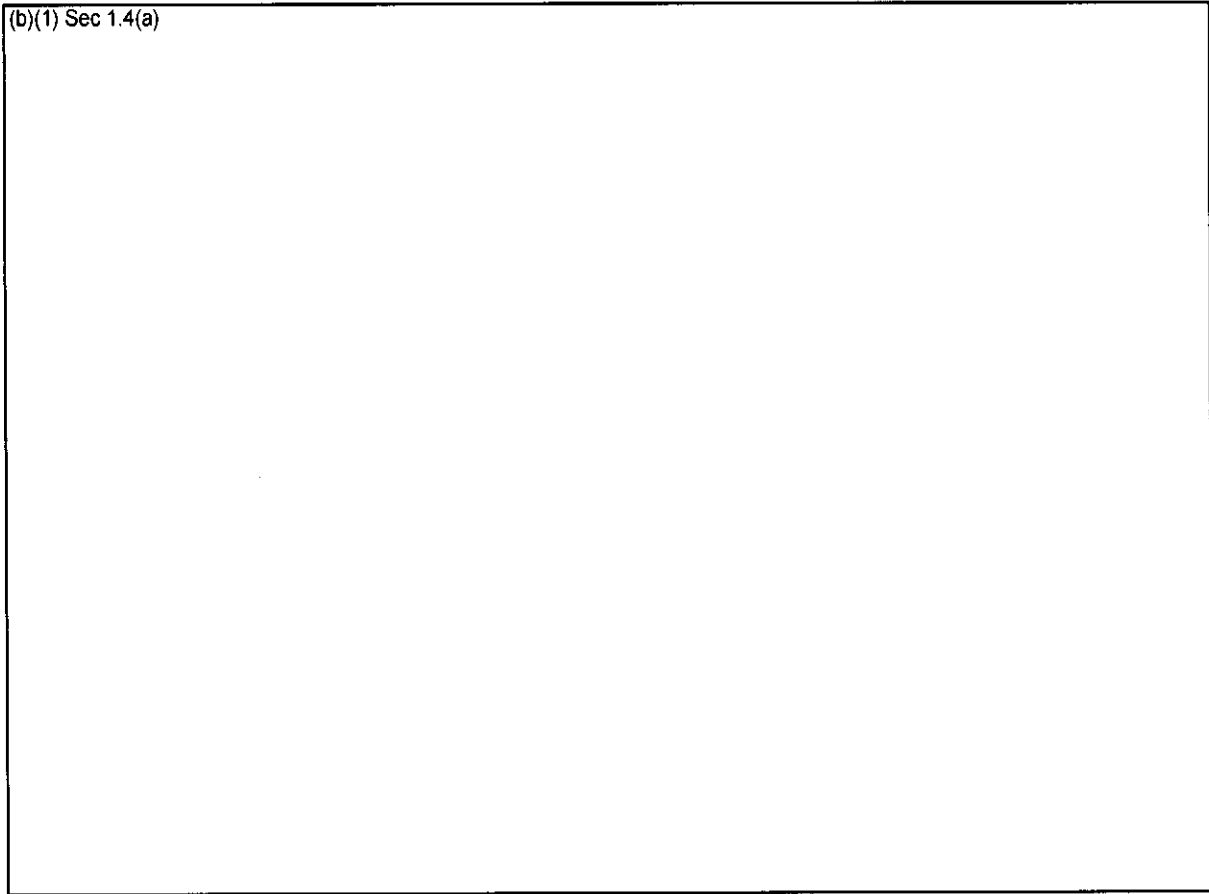
e. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The purpose of this  
(b)(1) Sec 1.4(a)

f. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) The supported Combatant  
Commander (b)(1) Sec 1.4(a)

g. (U) Figure C-18-2 below depicts the (b)(1) Sec 1.7(e)

SECRET

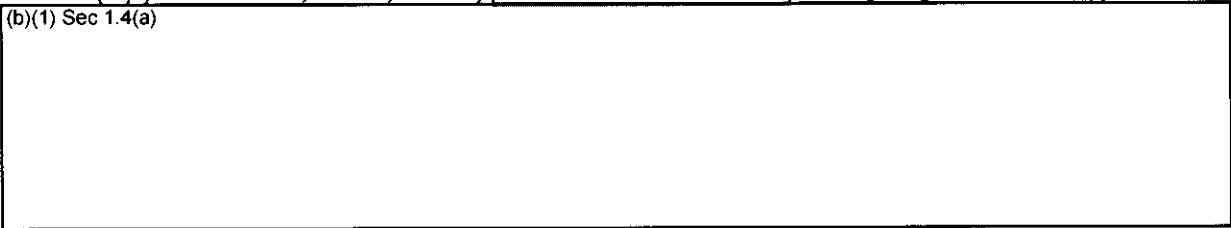
(b)(1) Sec 1.4(a)



83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103

(S//REL USA, AUS, GBR) Figure (C-18-1 - (b)(1) Sec 1.4(a)

c. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) The purpose of this (b)(1) Sec 1.4(a)



d. (U) (b)(1) Sec 1.7(e) The purpose of this (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) planning.

(1) (S//REL USA, AUS, GBR) JFCC GSI ICW the (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) USSTRATCOM operational recommendation. This recommendation will be presented for consideration to the Joint Staff and includes (b)(1) Sec 1.4(a)



USSTRATCOM recommendation for the way ahead.



SECRET

39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82

(b)(1) Sec 1.4(a)

a. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

establish/manage the planning timeline and expectations.

(1) (S//REL USA, AUS, GBR) GCCs and JFCC GSI continuously analyze current intelligence to determine if sufficient information exists (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

Combatant Commanders, other government agencies, and other planning partners in attendance. (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(2) (S//REL USA, AUS, GBR) A (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

provides initial tasks for participants, delineates the planning timeline and collaboration instructions, defines required products, (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

b. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) The purpose of this determining potential solutions.

(1) (S//REL USA, AUS, GBR) JFCC GSI conducts and leads mission analysis in a (b)(1) Sec 1.4(a)

Combatant Commands, Services, and participating USG agencies (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(2) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) JFCC GSI works with the supporting (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(3) (S//REL USA, AUS, GBR) Mission analysis will produce a (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
28 February 2008

1 APPENDIX 18 TO ANNEX C TO USSTRATCOM CONPLAN 8039(U)

2 (U) OPR: JFCC GSI J39      OCR: 8 IOF

3 (b)(1) Sec 1.7(e) FOR CYBERSPACE OPERATIONS (U)

4  
5 (U) References: See Base Plan and Annex C (Operations).

6  
7 (U)1. (~~S//REL USA, AUS, GBR~~) Situation

8  
9 a. (~~S//REL USA, AUS, GBR~~) General. (b)(1) Sec 1.4(a) is the  
10 process for producing USSTRATCOM recommended COAs (b)(1) Sec 1.4(a)  
11 (b)(1) Sec 1.4(a) or when directed by the Joint Staff (JS), for  
12 CDRUSSTRATCOM. This process is generally used for (b)(1) Sec 1.4(a)

13 (b)(1) Sec 1.4(a)  
14  
15  
16

17 executed by USSTRATCOM, (b)(1) Sec 1.4(a) and other organizations in order to  
18 facilitate synchronized and integrated effects. Several variables may dictate  
19 that the cyberspace operations (b)(1) Sec 1.4(a) differ from what is found in this  
20 appendix, (b)(1) Sec 1.4(a) in addition  
21 depending on interagency involvement, (b)(1) Sec 1.4(a)  
22 circumstances may be encountered. These situations will be handled on a by  
23 case basis. For example, (b)(1) Sec 1.4(a)

24 (b)(1) Sec 1.4(a)  
25  
26  
27  
28  
29  
30  
31  
32

33 commence planning and coordination with JFCC GSI.

34  
35 2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
36 (b)(1) Sec 1.4(a)  
37

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (e), and (g)~~  
~~Declassify on: 27 February 2033~~

38 (b)(1) Sec 1.4(a)

**SECRET**

40

41

(c) (U) Coordinate with DOD Components to determine the operational impact of changing DOD INFOCON levels.

43

44

(d) (U) Provide recommended changes to DOD INFOCON levels to CDRUSSTRATCOM.

45

46

47

4. (U) Administration and Logistics. Refer to Base Plan.

48

49

5. (U) Command and Control. Refer to Appendix 17 (NetOps) to Annex C (Operations).

50

**SECRET**

C-17-E-2

~~SECRET~~

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE NE 68113-6500  
28 February 2008

1 TAB E TO APPENDIX 17 TO ANNEX C TO CONPLAN 8039 (U)

2 (U) OPR: JTF-GNO J5

3 INFORMATION OPERATIONS CONDITION (INFOCON) (U)

4  
5 References: Refer to Base Plan and Appendix 17 (NetOps) to Annex C  
6 (Operations).

7  
8 1. (U) Situation. Refer to Base Plan.

9  
10 2. (U) Mission. Refer to Base Plan.

11  
12 3. (U) Execution

13  
14 a. (U) Concept of Operation. The INFOCON system, including  
15 responsibilities, processes and procedures, applies to all DOD information  
16 systems and networks operating at the Secret level (not to include closed,  
17 special enclave, or IC networks) and below under the purview of Office of the  
18 SECDEF, the Military Departments, the CJCS, The Combatant Commands,  
19 The Office of the Inspector General of the DOD, the Defense Agencies, the DOD  
20 Field Activities, and all other organizational entities within the Department of  
21 Defense hereafter referred collectively as the "DOD Components." The system  
22 also governs any interconnections between Public and DOD Unclassified  
23 networks, DOD Unclassified and Classified networks, and Classified and  
24 Classified networks.

25  
26 b. (U) Tasks

27  
28 (1) (U) CC/S/A will:

29  
30 (a) (U) Implement the INFOCON System IAW DODI-O 8530, CJCSI  
31 | 6510.01, Strategic Directive 527-1, and USSTRATCOM and JTF\_GNO guidance.

32  
33 | (2) (U) JTF\_GNO will:

34  
35 (a) (U) Monitor, track and provide global situational awareness on the  
36 Global INFOCON Indicators.

37  
38 (b) (U) Develop the execution guidance for implementation of the

~~Classified by: Multiple Sources~~

~~Reason: 1.4(a), (e), and (g)~~

~~Declassify on: 27 February 2033~~

39 INFOCON directive and incorporate it into NetOps plans.

~~SECRET~~

C-17-E-1

**SECRET**

(INTENTIONALLY BLANK)

**SECRET**  
C-17-D-4

# SECRET

85 (c) (U) Ensure that the DOD GIG is optimally delivering the  
86 information required by DOD GIG users in accordance with information  
87 delivery priorities.

88  
89 (d) (U) Ensure visibility of the information flowing across the DOD GIG  
90 and of those systems used to store, catalog, discover and transport  
91 information.

92  
93 (e) (U) Monitor information flows and access; determine impact to  
94 network capacity; and ensure that user profiles are being satisfied with a  
95 reasonable quality of service.

96  
97 (f) (U) Determine the sources responsible for providing information  
98 and stage information content throughout the DOD GIG in support of a given  
99 operation.

100  
101 (g) (U) Track and maintain knowledge of the various requests and user  
102 profiles for information; coordinate changes in the operating parameters of  
103 DOD GIG assets; identify new products; review and validate the user-profile  
104 database; and develop joint policies and procedures governing information flow  
105 across the DOD GIG.

106  
107 (2) (U) JTF GNO will:

108  
109 (a) (U) Direct GCM activities.

110  
111 (b) (U) Provide DOD GIG users with an awareness of relevant,  
112 accurate information and automated access to newly discovered information for  
113 timely, efficient delivery in a usable format.

114  
115 (c) (U) Provide guidance to capitalize on the content management  
116 framework found within the Net-Centric Enterprise Services (NCES) and Net-  
117 Centric Data Strategy.

118  
119 (d) (U) Facilitate the placement, posting and transport of information  
120 required by DOD GIG users.

121  
122 4. (U) Administration and Logistics. Refer to Base Plan.

123  
124 5. (U) Command and Control. Refer to Appendix 17 (NetOps) to Annex C  
125 (Operations).

SECRET

C-17-D-3

# SECRET

40 timely and efficient information delivery and/or search information databases  
41 to retrieve desired products as required.

42  
43 (4) (U) Improve bandwidth utilization.

44  
45 (5) (U) Enhance all aspects of the DOD GIG transport capabilities.

46  
47 b. (U) The core GCM services are Content Discovery, Content Delivery and  
48 Content Storage. These core services are envisioned to be enterprise wide  
49 services used by the entire DOD to ensure our information is available to all  
50 authorized users.

51  
52 (1) (U) Content Discovery. Content Discovery provides the ability to  
53 quickly search for information throughout the DOD GIG. Using any appropriate  
54 web browser, whether on a desktop computer or wireless device, operational  
55 staffs can search across multiple sources from one place, vice making several  
56 attempts. Once the product is located, the Content Delivery service permits the  
57 users to pull in the needed product.

58  
59 (2) (U) Content Delivery. Information that is requested by a DOD GIG  
60 user is delivered using the GCM delivery service. Content Delivery provides the  
61 user the capability to replicate files and directives, publish and subscribe to  
62 information based on roles and responsibilities, and provide assured, timely  
63 transport of the information to include notification of when the information was  
64 read by a distant user. Items are delivered across multiple, heterogeneous  
65 communication systems with delivery and read receipt notifications, providing  
66 assured delivery of information products.

67  
68 (3) (U) Content Storage. Content Storage provides physical and virtual  
69 places to host data on the network with varying degrees of persistence. These  
70 information storage capabilities will be located throughout the DOD GIG.

71  
72 c. (U) Tasks. CDRUSSTRATCOM, through the JTF\_GNO and the NetOps  
73 Community, directs GCM through the policies, procedures, programs, and  
74 operations that prepare DOD systems, networks and personnel to manage the  
75 content of the DOD GIG, and coordinates with the interagency as required.

76  
77 (1) (U) CC/S/A will:

78  
79 (a) (U) Act on JTF GNO direction with regard to GCM activities.

80  
81 (b) (U) Ensure the Content Discovery, Storage, and Delivery services  
82 as well as mitigation are operating correctly and that information is  
83 "maneuvered" to the optimum location on the DOD GIG.

84

# SECRET

C-17-D-2

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE NE 68113-6500  
28 February 2008

1 TAB D TO APPENDIX 17 TO ANNEX C TO CONPLAN 8039 (U)

2 (U) OPR: JTF-GNO J5

3 GIG CONTENT MANAGEMENT (GCM) (U)

4  
5 References: See Base Plan and Appendix 17 (NetOps) to Annex C (Operations).

6  
7 1. (U) Situation. Refer to Base Plan.

8  
9 2. (U) Mission. Refer to Base Plan.

10  
11 3. (U) Execution

12  
13 a. (U) Concept of Operations. GCM is the essential task that ensures  
14 information is available on the DOD GIG. At any time within the DOD GIG,  
15 there are information consumers and producers, who either publish or access  
16 the information required to accomplish their mission. Information exists in file  
17 sizes ranging from kilobytes to terabytes, all of which must be identifiable and  
18 accessible to appropriate users. GCM enables information users to define and  
19 set information needs to facilitate timely information delivery and to search  
20 information databases and retrieve required products. GCM maneuvers  
21 information across the DOD GIG, focusing on positioning and re-positioning of  
22 content to the optimum location in order to satisfy mission needs. This  
23 essential task adjusts information delivery methods and priorities for enhanced  
24 SA, and allows information producers to advertise, publish and distribute  
25 information. GCM is accomplished by enabling DOD GIG users to safeguard,  
26 compile, catalog, discover, cache, distribute, retrieve and share data in a  
27 collaborative environment. GCM will allow NetOps centers to optimize the flow  
28 and location of information over the DOD GIG by positioning and repositioning  
29 data and services to optimum locations on the DOD GIG in relation to the  
30 information producers, information consumers, and the mission requirements.  
31 Some of the objectives of GCM are:

32  
33 (1) (U) Enable commanders to adjust information delivery methods and  
34 priorities for enhanced SA.

35  
36 (2) (U) Enable information producers to advertise, publish, and distribute  
37 information to the warfighter.

38  
39 (3) (U) Enable users to define and set information needs to facilitate

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (e), and (g)~~  
~~Declassify on: 27 February 2033~~

**SECRET**

C-17-D-1



**SECRET**

(INTENTIONALLY BLANK)

**SECRET**  
C-17-C-4

# SECRET

85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102

(e) (U) Direct RA and coordinate with network warfare mission partners, JFCC NW, and others as appropriate IAW CJCSI 3121.01B.

(f) (U) Coordinate with LE/CI for investigation of the malicious activity.

(g) (U) Validate and prioritize identified critical assets meeting established CIP criteria, and ensure remediation, mitigation, and reconstitution plans are developed and maintained by asset owners.

(h) (U) Establish standards and programs for GIG management and defense, training, awareness, and certification across DOD IAW OSD policy and USSTRATCOM direction.

4. (U) Administration and Logistics. Refer to the Base Plan.

5. (U) Command and Control. Refer to the Base Plan and Annex J (Command Relationships).

# SECRET

39 (d) (U) Alert others on the GIG of local incident status to correct the  
40 intrusion.

41  
42 (e) (U) Certify, accredit and report on all networks, peripherals, and  
43 edge devices in their portion of the GIG in addition to enforcing information  
44 security (INFOSEC).

45  
46 (f) (U) Conduct security readiness reviews and vulnerability analysis  
47 assessments of subordinate units for compliance with CTOs and IAVAs and  
48 report compliance to JTF\_GNO.

49  
50 (g) (U) Ensure compliance of GIG management and defense training,  
51 awareness and certification programs per established policies and directives.

52  
53 (h) (U) Develop and deconflict local contingency plans to defend  
54 against malicious activity in their portion of the GIG and provide copies to JTF  
55 GNO.

56  
57 (i) (U) Conduct risk assessment of their networks.

58  
59 (j) (U) Share GND information with Allies and coalition partners in  
60 accordance with formal agreements and national disclosure policies except  
61 where limited by law, policy, or security classification.

62  
63 (k) (U) Provide reporting as tasked.

64  
65 (l) (U) Develop and maintain remediation, mitigation and  
66 reconstitution plans for CIP criteria.

67  
68 (2) (U) JTF GNO

69  
70 (a) (U) Direct GND activities.

71  
72 (b) (U) Notify the NetOps Community of ongoing or developing threats  
73 and anomalies via SA Reports, IAVAs, or Information Assurance Vulnerability  
74 Bulletins (IAVBs) and reduce potential risks by issuing CTOs and/or  
75 conducting a Significant Event Conference (SIEC).

76  
77 (c) (U) Provide guidance and execution instructions for managing and  
78 increasing OPSEC control measures for the GIG and NetOps Community in  
79 response to the identified threat level.

80  
81 (d) (U) Assess the possible impact the anomaly or incident will have on  
82 the rest of the GIG. JTF\_GNO will direct GND activities and actions in  
83 accordance with the defined NetOps C2 construct. The NetOps Community will  
84 manage its affected portions of the GIG through local procedures (JTTPs).

SECRET

C-17-C-2

**SECRET**

HEADQUARTERS, U.S. STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE NE 68113-6500  
28 February 2008

1 TAB C TO APPENDIX 17 TO ANNEX C TO CONPLAN 8039 (U)

2 (U) OPR: JTF-GNO J5

3 GIG NETWORK DEFENSE (GND) (U)

4  
5 References: Refer to Base Plan.

6  
7 1. (U) Situation. Refer to Base Plan.

8  
9 2. (U) Mission. Refer to Base Plan.

10  
11 3. (U) Execution

12  
13 a. (U) Concept of Operations

14  
15 (1) (U) GND activities consist of the policies, procedures, programs and  
16 operations that prepare DOD systems, networks and personnel to protect the  
17 GIG, as well as coordination with the interagency as required.

18  
19 (2) (U) CDRUSSTRATCOM, through JTF\_GNO and the NetOps  
20 Community, directs GND.

21  
22 (3) (U) GIG constituent systems that meet the definition of a National  
23 Security System (NSS) must follow the appropriate Information Assurance (IA)  
24 guidelines and policies for NSS in accordance with the National Manager for  
25 NSS. Other GIG systems not designated NSS must be provided adequate IA to  
26 not jeopardize the security of GIG NSS systems.

27  
28 b. (U) Tasks

29  
30 (1) (U) CC/S/A will:

31  
32 (a) (U) Act on JTF\_GNO direction with regard to GND.

33  
34 (b) (U) Detect and perform analysis of an anomaly or intrusion,  
35 providing JTF\_GNO with incident reports through their GND Tier Structure.

36  
37 (c) (U) Direct RA in their portion of the GIG IAW CJCSI 3121.01B.

38  
~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (e), and (g)~~  
~~Declassify on: 06 December 2032~~

**SECRET**

C-17-C-1

~~SECRET~~

135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156

INTENTIONALLY BLANK

~~SECRET~~

C-17-B-4

# SECRET

- 91 4. (U) Administration and Logistics. Refer to Base Plan.  
92  
93 | 5. (U) Command and Control. Refer to Appendix 17 (NETOPS).  
94

95  
96  
97  
98  
99

100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134

SECRET

**SECRET**

47 (5) (U) Electromagnetic Spectrum Management. Ensures combatant  
48 commanders and subordinate commanders are aware of spectrum  
49 management decisions that impact mission accomplishment, and provides for  
50 efficient employment of the electromagnetic spectrum in terms of planning,  
51 allocation, coordination with other spectrums, interference resolution, and

52 (b)(1) Sec 1.7(e)

53  
54 | b. (U) Tasks. CDRUSSTRATCOM, through JTF\_GNO and the NetOps  
55 community, directs GEM through the policies, procedures, programs, and  
56 operations that prepare DOD systems, networks and personnel to manage the  
57 DOD GIG, and coordinates with the interagency as required.

58  
59 (1) (U) CC/S/A will:

60  
61 | (a) (U) Act on JTF\_GNO direction with regard to GEM.

62  
63 (b) (U) Report outages, degradations, and upgrade operations having  
64 an operational impact on GIG functionality.

65  
66 (c) (U) Monitor and adjust their portion of the DOD GIG to ensure its  
67 health and integrity (in accordance with Information Assurance Control  
68 Implementation guides).

69  
70 (d) (U) Build and maintain SA over their portion of the DOD GIG.

71  
72 (e) (U) Report network outages, degradations, and upgrade operations  
73 having an operational impact on the DOD GIG functionality using the CND Tier  
74 structure.

75  
76 (f) (U) Maintain robust and redundant DOD GIG capability.

77  
78 (g) (U) Develop, as necessary, standardized local procedures to  
79 | implement JTF\_GNO guidance (e.g., Joint Tactics, Techniques and Procedures  
80 (JTTPs)).

81  
82 | (2) (U) JTF GNO will:

83  
84 (a) (U) Direct GEM activities.

85  
86 (b) (U) Build and maintain SA over the DOD GIG infrastructure.

87  
88 (c) (U) Report outages, degradations, and upgrade operations having  
89 an operational impact on the DOD GIG.

90  
**SECRET**

# SECRET

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE NE 68113-6500  
28 February 2008

1  
2  
3  
4  
5  
6 TAB B TO APPENDIX 17 TO ANNEX C TO CONPLAN 8039 (U)

7 (U) OPR: JTF-GNO J5

8 GIG ENTERPRISE MANAGEMENT (GEM) (U)

9  
10 References: Refer to Appendix 17 (NetOps).

11  
12 1. (U) Situation. Refer to Base Plan.

13  
14 2. (U) Mission. Refer to Base Plan.

15  
16 3. (U) Execution

17  
18 a. (U) Concept of Operations. GEM encompasses the DOD GIG's IT services  
19 management. This consists of the many elements and processes needed to  
20 communicate across the full spectrum of the DOD GIG, and include the  
21 following:

22  
23 (1) (U) Enterprise Services Management. Provides services for end-user  
24 applications, web-based services, remote hosted applications, discovery,  
25 storage, software applications and other IT components of applications.

26  
27 (2) (U) Systems Management. Comprises all measures necessary to  
28 ensure the effective and efficient operations of GIG information systems,  
29 elements of systems, and services. Provides day-to-day management of  
30 information systems, elements of systems, and services to include operating  
31 systems, databases, and hosts of the end-users.

32  
33 (3) (U) Network Management. Provides networked system services with  
34 the desired level of quality and guaranteed availability. Networks use all  
35 available means of communication including terrestrial, airborne and/or  
36 satellite, and include: switched networks, data networks, Video  
37 Teleconferencing (VTC) networks, satellite networks and wireless networks.

38  
39 (4) (U) Satellite Communications Management. Provides day-to-day  
40 operational management of all apportioned and non-apportioned SATCOM  
41 resources, to include appropriate support when disruption of service occurs.  
42 This includes global SATCOM system status and maintains global SA to  
43 include each combatant commander's current and planned operations as well  
44 as Space, Control, and Terminal Segment asset and operational configuration  
45 management.

46  
**SECRET**

C-17-B-1



~~SECRET~~

161

INTENTIONALLY BLANK

~~SECRET~~  
C-17-A-6

**SECRET**

120 (f) (U) Non-DOD NETOPS activities will be executed per memorandum of  
121 agreement with the DOD.

122  
123 c. (U) Tasks: JTF-GNO will:

124  
125 (1) (U) Direct the operations and defense of the DOD GIG with the  
126 authority and responsibilities assigned by the President, SECDEF and  
127 CDRUSTRATCOM and is thereby empowered to order actions that execute  
128 directions given.

129  
130 (2) (U) Ensure both the operational and functional chains of command are  
131 included in JTF-GNO orders.

132  
133 (3) (U) Ensure that NETOPS activities are executed at the lowest level of  
134 command possible within the NETOPS Community.

135  
136 (4) (U) Use the decision matrix (Figure C-17-A-4) to help determine if the  
137 NETOPS incident is a global event. A "yes" answer to any of these four criteria  
138 may drive the incident to be "fought" at a "global" level.

139  
140 (a) (U) An incident crosses a Geographic Combatant Command (GCC)  
141 boundary.

142  
143 (b) (U) An incident affects multiple combatant commanders.

144  
145 (c) (U) An incident impacts multiple DOD agency enterprises.

146  
147 (d) (U) An incident is beyond a combatant commander's capabilities.

148

Criteria Incident	CROSSES THEATER BOUNDARY	IMPACTS MULTIPLE COCOMS	IMPACTS OTHER AGENCIES	BEYOND THEATER CAPABILITIES	GLOBAL EVENT?

149

150

151

152

153

154

155

156

157

158

159

160

Figure C-17-A-4: Decision Matrix (U)

4. (U) Administration and Logistics. See Base Plan.

5. (U) Command and Control. Refer to Appendix 17 (NETOPS)

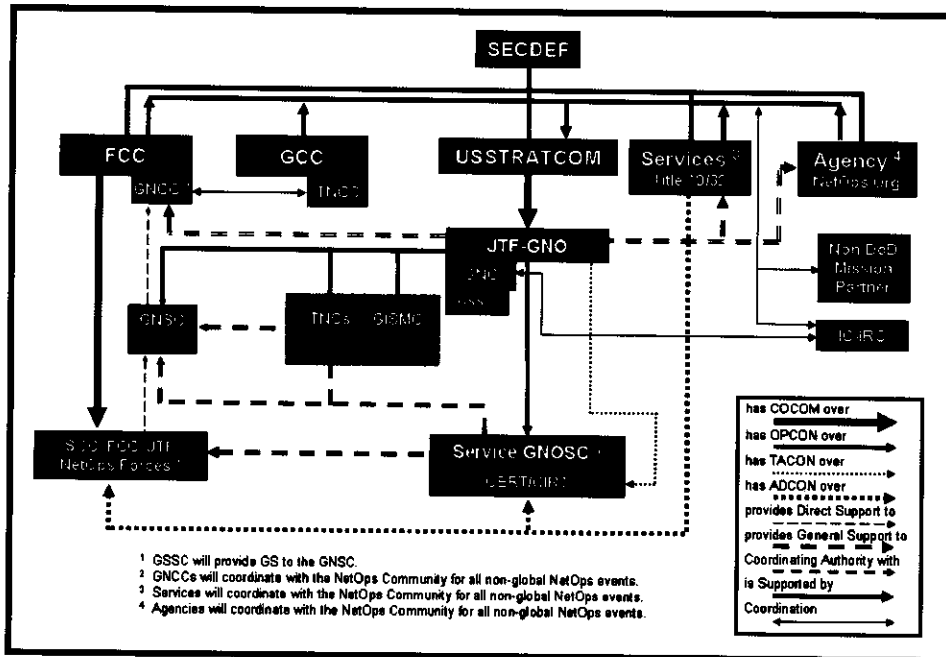


Figure C-17-A-3: Non-Global NETOPS C2 with USSTRATCOM as Supported Command (U)

(a) (U) The supported commander has the authority to take whatever NETOPS action is deemed necessary, to support the mission and has final decision responsibility.

(b) (U) The establishing authority (CDRUSSTRATCOM) will outline the generic responsibilities of the supported and supporting commanders as they apply to NETOPS during global, theater, and the non-global NETOPS events.

(c) (U) Simultaneous collaboration, both vertically and horizontally, is fundamental to SA and is vital in determining the impact of an incident (global, theater or non-global).

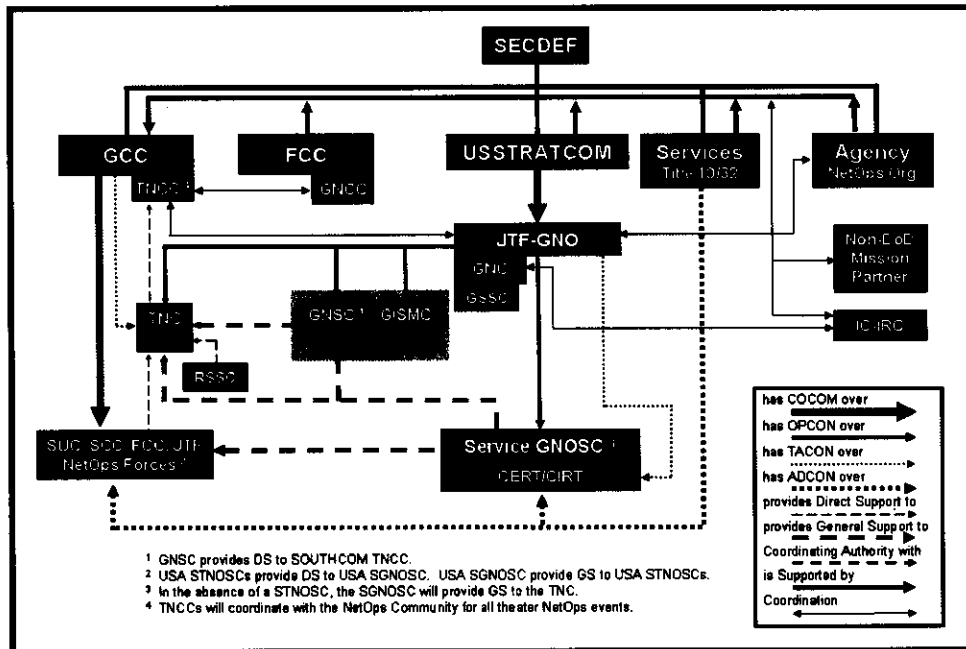
(d) (U) In time-critical situations, such as when an immediate Network Defense (ND) action is warranted to defend the DOD GIG within an area of responsibility (AOR), action may be initiated by the supported CC/S/A prior to collaborating or collaboration may be abbreviated. Collaboration must then follow, in order to mitigate or remediate global affects, if any.

(e) (U) NETOPS activities affecting (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

73 (2) (U) Supporting Command. CDRUSSTRATCOM is the supporting  
 74 commander when designated by the SECDEF in an EXORD or when executing a  
 75 mission for NETOPS events that are not deemed global or non-global by CDR,  
 76 JTF-GNO per authority delegated by CDRUSSTRATCOM (see Figure C-17-A-2).  
 77 COCOMs, JTF-GNO, JTF-GNO Service NETOPS Components, FCCs, and  
 78 Agencies shall provide support to the affected CC/S/A for theater NETOPS  
 79 events. Non-DOD U.S. government (USG) organizations, intergovernmental  
 80 organizations (State and Local), non-governmental organizations (NGO),  
 81 multinational military commands (alliances and coalitions), as well as  
 82 commercial and research communities may also provide support per inter-  
 83 governmental agreements. Most NETOPS events begin as theater events in a  
 84 local enclave that are under the control of the respective GCC. Theater NETOPS  
 85 events are those activities occurring within a theater that have the potential to  
 86 impact the operations in that theater.

87  
 88

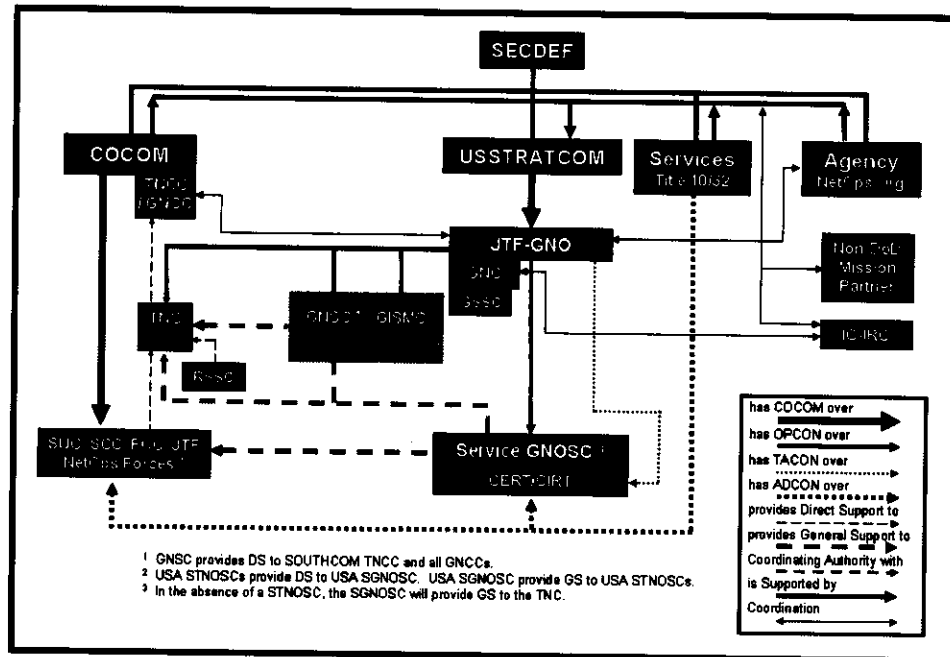


89  
 90  
 91

Figure C-17-A-2: Theater NETOPS C2 with GCC as Supported Command (U)

SECRET

45 mission while operating and defending against NETOPS events that have a global  
 46 or non-global impact (see Figures C-17-A-1 and C-17-A-3). CDR, JTF-GNO, via  
 47 delegated authority from CDRUSSTRATCOM, will determine when a network  
 48 incident requires him/her to assume this role. In such circumstances, CDR,  
 49 JTF-GNO, will issue orders and direction with the authority of  
 50 CDRUSSTRATCOM, to the CC/S/As and other stakeholders with connection to  
 51 the DOD GIG to ensure availability and integrity of the DOD GIG. While this  
 52 supported relationship gives CDRUSSTRATCOM global authority, it does not  
 53 negate the COCOM's authority over NETOPS forces as specified in the UCP, 5  
 54 May 06. JTF-GNO Service NETOPS Components will support the execution of  
 55 operating and defending against global and non-global NETOPS events, while  
 56 synchronizing actions with affected COCOMs and their respective Components.  
 57 Global NETOPS events are those activities that have the potential to impact the  
 58 operational readiness of the DOD GIG and require a coordinated response  
 59 amongst CC/S/As. CC/S/As are responsible for leading their respective  
 60 responses to global NETOPS events in accordance with USSTRATCOM and JTF-  
 61 GNO direction. Non-global NETOPS events are those activities whose impact  
 62 affects FCCs, unassigned Title 10 Service forces, or Defense Agencies and are  
 63 neither global nor theater in nature. JTF-GNO will provide GS to the FCCs,  
 64 Services, and Agencies for non-global NETOPS events. USSTRATCOM and JTF-  
 65 GNO, in conjunction with CC/S/As, will establish JTTPs that provide specifics  
 66 for executing the supported/supporting relationships with regard to global  
 67 NETOPS events.



68  
 69  
 70  
 71  
 72

Figure C-17-A-1: Global NETOPS C2 with USSTRATCOM as Supported Command (U)

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE NE 68113-6500  
28 February 2008

1  
2 TAB A TO APPENDIX 17 TO ANNEX C TO CONPLAN 8039-07 (U)

3 (U) OPR: JTF-GNO J5

4 NETOPS COMMAND AND CONTROL (C2) (U)

5  
6 References: See Appendix 17 (NETOPS) to Annex C (Operations)

7  
8 1. (U) Situation. See Base Plan.

9  
10 2. (U) Mission. See Base Plan.

11  
12 3. (U) Execution

13  
14 a. (U) Concept of Operations. In order to execute its UCP missions,  
15 CDRUSSTRATCOM delegates operational and tactical level planning, force  
16 execution, and day-to-day force management to JFCCs, Task Forces (TF), and  
17 Centers. These JFCCs, TFs, and Centers conduct operations for USSTRATCOM  
18 while the Headquarters focuses on strategic-level integration and advocacy of its  
19 assigned missions. At the request of CDRUSSTRATCOM, the SECDEF assigned  
20 the Director, Defense Information Systems Agency (DISA) as Commander, JTF-  
21 GNO, with authorities and responsibilities for Global Network Operations and  
22 Defense. Global NETOPS is conducted by JTF-GNO, unless otherwise directed  
23 by CDRUSSTRATCOM. Such operations include apprising CDRUSSTRATCOM  
24 on NETOPS matters impacting the DOD GIG's integrity and support of DOD  
25 missions. CDR, JTF-GNO, via delegated authority from CDRUSSTRATCOM,  
26 manages the apportionment and allocation of GIG system and network  
27 resources.

28  
29 b. (U) NETOPS. NETOPS faces the same set of hierarchical C2 complexities  
30 as any other joint force operation. To facilitate net-centricity, NETOPS must  
31 adopt new Information Age C2 structures and processes that breed self-  
32 synchronized support for effective operations and defense of the DOD GIG.  
33 Today, rapidly changing technology and a lack of acquisition standardization  
34 challenges effective operation and defense of the DOD GIG from one centralized  
35 headquarters. Thus, effective operation and defense of the DOD GIG requires  
36 trained and certified NETOPS operators at all levels, with a common purpose,  
37 vision, and understanding of CDRUSSTRATCOM's intent. Until technology  
38 advances, JTF-GNO, in concert with Combatant Commands, Services and  
39 Agencies (CC/S/As) will develop full situational awareness of the DOD GIG  
40 through common processes, standards and instrumentation, enabling near real  
41 time manipulation of any asset in order to optimize net-centric services.

42  
43 (1) (U) Supported Command. CDRUSSTRATCOM is the supported  
44 commander when designated by the SECDEF in an EXORD or when executing a

**SECRET**

C-17-A-1

~~SECRET~~

- 204 C - GIG Network Defense (GND)
- 205 D - GIG Content Management (GCM)
- 206 E - Information Operations Conditions (INFOCONS)
- 207

~~SECRET~~

# SECRET

158  
159 (2) (U) Assured information protection offers digital, electronic, and  
160 cognitive protection to counter attacks against US interests in cyberspace. For  
161 example, GND and GCM activities include information assurance and  
162 protection of data.

163  
164 (3) (U) Assured information delivery offers cyber and cognitive protection  
165 to counter attacks against US interests in cyberspace. For example, GCM and  
166 GEM activities include the optimization of information flow and location and  
167 maintaining redundant GIG capabilities.

168  
169 (4) (U) The synergy achieved through the layering of NetOps Effects  
170 provides defense in depth for the (b)(1) Sec 1.7(e)  
171 (b)(1) Sec 1.7(e).

172  
173 c. (U) NetOps Support to (b)(1) Sec 1.7(e) NetOps Effects ensure support  
174 (b)(1) Sec 1.7(e)

175  
176 d. (U) Tasks

177  
178 (1) (U) CC/S/A are required to perform the essential tasks of GEM (See  
179 TAB B), GND (TAB C), and GCM (TAB D). Adhering to the responsibilities of  
180 the essential tasks (GEM, GND, and GCM) produces NetOps' desired effects of:  
181 Assured System and Network Availability, Assured Information Protection, and  
182 Assured Information Delivery in support of the overall goal of NetOps. NetOps  
183 and its essential tasks GEM, GND, and GCM include IA and can only occur  
184 when IA measures are implemented and accomplished within the GIG.

185  
186 (2) (U) JTF GNO directs the operation and defense of the GIG to ensure  
187 timely and net-centric capabilities across strategic, operational, and tactical  
188 boundaries in support of the full spectrum of business, intelligence and  
189 warfighting. Specific responsibilities for the JTF GNO include establishing SA,  
190 developing NetOps tactics, identifying GIG measures of effectiveness,  
191 publishing plans and orders, coordinating RA to attacks against the GIG, and  
192 conducting network threat intelligence.

193  
194 4. (U) Administration and Logistics. Not used.

195  
196 5. (U) Command and Control. For NetOps Command and Control, refer to Tab  
197 A (NetOps Command and Control).

198  
199  
200  
201 Tabs

- 202 A – NetOps Command and Control (C2)  
203 B – GIG Enterprise Management (GEM)

SECRET

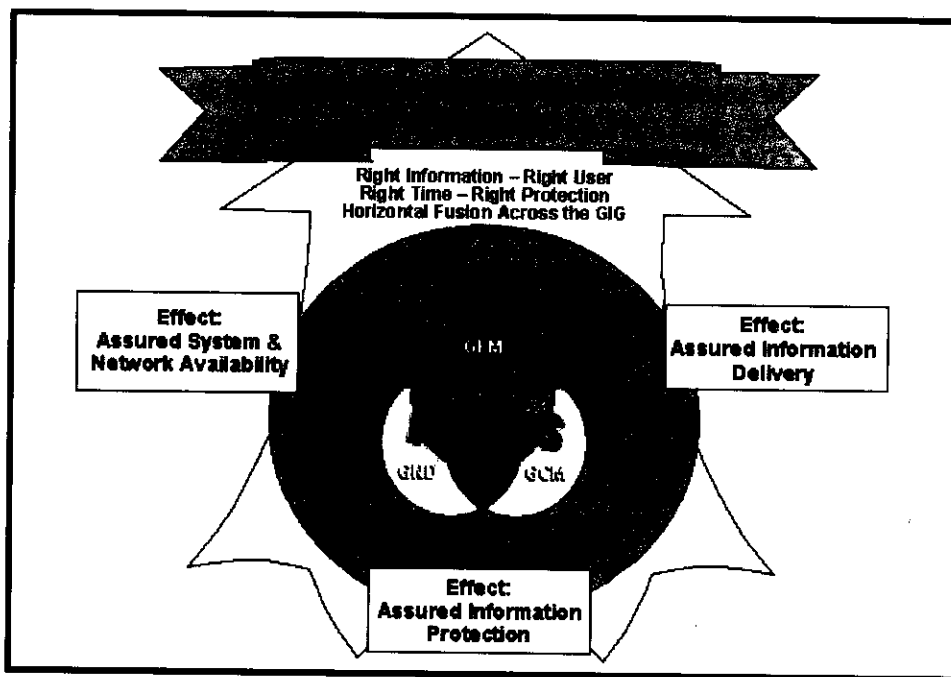


131 essential tasks. Each effect is further described in the following bullets and the  
132 relation of the essential tasks and effects are depicted below in Figure C-17-1.  
133

134 (1) (U) Assured System and Network Availability is achieved through  
135 visibility and control over the system and network resources. Resources are  
136 managed and problems are anticipated and mitigated, ensuring uninterrupted  
137 availability and protection of the system and network resources. This includes  
138 providing for graceful degradation, self-healing, fail over, diversity, and  
139 elimination of critical failure points.  
140

141 (2) (U) Assured Information Protection applies to information in  
142 storage/at rest, as well as passing over networks, from the time it is stored and  
143 cataloged, until it is distributed to the users, operators and decisions makers.  
144

145 (3) (U) Assured Information Delivery provides information to users,  
146 operators and decision makers in a timely manner.  
147



148  
149 (U) Figure C-17-1: Relation of Essential Tasks, Effects, and NetOps  
150

151 c. (U) NetOps Support (b)(1) Sec 1.7(e) The achievement of NetOps Effects ensures  
152 (b)(1) Sec 1.7(e)

153  
154 (1) (U) Assured system and network availability offers digital, electronic,  
155 and physical protection to counter attacks against US interests in cyberspace.  
156 For example, GEM and GND activities include the reporting of anomalies  
157 affecting GIG health and critical infrastructure protection.

**SECRET**

85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130

3. (U) Execution. The execution of NetOps remains the same throughout the

(b)(1) Sec 1.7(e)

a. (U) Concept of Operations. NetOps is defined as the operational framework consisting of three essential tasks, SA, and C2 that CDRUSSTRATCOM, in coordination with the NetOps Community, employs to operate and defend the GIG to ensure information superiority. The GIG is a globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The three essential tasks are GIG Enterprise Management (GEM), GIG Network Defense (GND), and GIG Content Management (GCM). The synergy achieved by each integrated relationship between any two of the essential tasks (GEM, GND, and GCM) produces NetOps' desired effects of: Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery in support of the overall goal of NetOps, which is to provide the right information to the edge. NetOps and its essential tasks GEM, GND, and GCM includes IA as defined and outlined in DODD 8500.1, Information Assurance, and CJCSI 6510.01D, Information Assurance and Computer Network Defense. Successful NetOps can only occur when IA measures are implemented and accomplished within the GIG. USSTRATCOM will organize its forces, identify mission essential tasks and training requirements, measure and report readiness, and direct the operation and defense of the GIG IAW the Joint CONOPS for GIG NetOps. CDRUSSTRATCOM exercises C2 through the JTF GNO. Successful operation and defense of the GIG requires an adaptive force comprised of professionals at the JTF GNO and throughout the NetOps Community. The NetOps Community is defined as the GIG providers, operators, defenders, and subscribers who possess a fundamental understanding of their responsibilities, and act synchronously to support DOD and NetOps mission partners' missions and operations. The community members include but are not limited to NetOps organizations in the CC/S/A who install, operate, maintain and defend the GIG as described in DODD 8100.1. However, it also includes major contributors to NetOps such as the OSD, Joint Staff J6, the IC Incident Response Center (IC-IRC) and (b)(1) Sec 1.7(e)

b. (U) NetOps Effects. The desired effects of NetOps are as follows: Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery. Two key principles must be applied to achieve the three desired effects: essential tasks must be performed interdependently (i.e. GND cannot be performed separately from GEM as the two are synergistically coupled and are essential to evoking GCM), and JTF GNO in collaboration with the NetOps Community must perform the responsibilities associated with each essential task processes. These three effects of NetOps are derived through the synergy achieved by each integrated relationship between any two of the

**SECRET**

- 39
- 40 m. (U) DODD 8500.1, Information Assurance (IA), 21 Nov 03
- 41
- 42 n. (U) DODD O-8530.1, Computer Network Defense, 8 Jan 01
- 43
- 44 o. (U) DODI 8100.dd, NetOps for the GIG – DRAFT
- 45
- 46 p. (U) DODI O-8530.2, Support to Computer Network Defense (CND), 9 Mar
- 47 01
- 48
- 49 q. (U) ASD NII/DOD CIO and IC CIO MOA, Sharing Network Management
- 50 and Computer Network Defense Information, 24 Jul 05
- 51
- 52 r. (U) Joint USSTRATCOM/ASD NII Memorandum, Computer Network
- 53 Defense Strategy for Defense in Depth in Support of the DOD IO Roadmap, 13
- 54 Jan 05
- 55
- 56 s. (U) Joint Command and Control Functional Concept, Feb 04, p. 32
- 57
- 58 t. (U) JTF GNO OPORD 05-01 (Global Network Operations), 7 Feb 05
- 59
- 60 u. (U) JTF GNO TTX-1 VTC Minutes, 14 Nov 05
- 61
- 62 v. (U) JTF GNO TTX-2 Conference Minutes, 15 Dec 05
- 63
- 64 w. (U) JTF GNO Strategic Plan, An Adaptive Force Ensuring Information
- 65 Delivery, Feb 06
- 66
- 67 x. (U) Joint Functional Component Command Space and Global Strike
- 68 Concept of Operations, 1 Jan 06, DRAFT
- 69
- 70 y. (U) JFCC SGS CONOPS, 1 Jun 06 Draft NSD-42 National Policy for the
- 71 Security of National Security Telecommunications and Information Systems,
- 72 signed by the President on 5 Jul 90
- 73
- 74 z. (U) SD 527-1, DOD Information Operations Condition (INFOCON)
- 75 System Procedures, 27 Jan 06
- 76
- 77 1. (U) Situation
- 78
- 79 a. (U) (b)(1) Sec 1.7(e)
- 80 (b)(1) Sec 1.7(e)
- 81
- 82 b. (U) Friendly. NetOps forces. Refer to Annex A (Task Organization).
- 83
- 84 2. (U) Mission. Refer to Base Plan.

**SECRET**

C-17-2

# SECRET

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE NE 68113-6500  
28 February 2008

1 APPENDIX 17 TO ANNEX C TO STRATCOM CONPLAN 8039-07 (U)

2 (U) OPR: JTF-GNO J5

3 NETOPS (U)

4  
5 References: Refer to Base Plan.

6  
7 a. (U) SECDEF Memo, Forces For Unified Commands Memorandum, FY06  
8 (S), 15 Feb 06

9  
10 b. (U) DEPSECDEF Guidance and Policy Memo 10-8460

11  
12 c. (U) USSTRATCOM Memo, Delegation of Authorities to Director, Defense  
13 Information Systems Agency (DISA), 30 Sep 03

14  
15 d. (U) USSTRATCOM Memo, SECDEF Appointment of the Person Serving  
16 as Director, Defense Information Systems Agency (DISA), as Commander, Joint  
17 Task Force – Global Network Operations (JTF-GNO), 21 Jun 05

18  
19 e. (U) USSTRATCOM Network Warfare Concept of Operations- Final, Mar  
20 06

21  
22 f. (U) USSTRATCOM Integrating Guidance DRAFT, 19 Dec 05

23  
24 g. (U) CJCSI 6215.03, GIG Network Operations – DRAFT, Nov 05

25  
26 h. (U) CJCSI 6510.01D, Information Assurance (IA) and Computer Network  
27 Defense (CND) (U), 15 Jun 04

28  
29 i. (U) CJCSM 3402.01B, Alert System of the Chairman of the Joint Chiefs  
30 of Staff (U), 1 Nov 00

31  
32 j. (U) DODD 8100.1, Global Information Grid Overarching Policy, 21 Nov  
33 03

34  
35 k. (U) DODD 3020.40, Defense Critical Infrastructure Program, 19 Aug 05

36  
37 l. (U) DODD O-5100.30, Department of Defense Command and Control, 5

~~Classified by: Multiple Sources~~

~~Reason: 1.4(a), (e), and (g)~~

~~Declassify on: 06 December 2032~~

38 Jan 06

SECRET

C-17-1

**SECRET**

248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271

(b) (~~S//REL USA, AUS, GBR~~) USSTRATCOM not being able to meet

(b)(1) Sec 1.4(a)

(c) (U) USSTRATCOM personnel death or involvement in the death of another or death or serious illness of high-level government official.

(d) (U) A significant degradation to CI supporting a USSTRATCOM mission.

(3) (U) (b)(1) Sec 1.7(e) Report any indications of:

(a) (U) Substantial degradation in US communications capabilities, SATCOM, Terrestrial, Communications Relay System, or ground station that is part of the Communications Network.

(b) (U) Imminent or direct attacks/intrusions against the GIG and/or Coalition/Allied networks.

(4) (U) Essential Elements of Friendly Information (EEFIs). Report:

(a) (U) Discovery of a significant unmitigated vulnerability to the GIG.

**SECRET**

202 (3) (U) Commanders will initiate a report through the chain of command  
203 for any of the following incidents impacting critical infrastructure supporting  
204 this OPLAN.

205  
206 (a) (U) Initiation of an infrastructure incident response plan.

207  
208 (b) (U) Potential or actual use of WMD against DOD assets or  
209 infrastructure.

210  
211 (c) (U) Threat Information Report specifically related to infrastructure.

212  
213 d. (U) Data Collection and Reporting. Collect as much information as  
214 possible for initial notification reporting, but do not delay notification to gather  
215 complete data. Submit all reports as soon as possible after an event or  
216 incident has occurred in accordance with the USSTRATCOM JTF\_GNO (b)(1) Sec 1.7(e)  
217 Reporting Matrix dated 1 May 07. Use all sources, including host nation  
218 agencies, to gather data (i.e., who, what, when, where, why, how).

219  
220 (1) (~~S//REL USA, AUS, GBR~~) USSTRATCOM (b)(1) Sec 1.4(a)  
221 (b)(1) Sec 1.4(a) notification to  
222 Commander, USSTRATCOM and senior staff. This may include (b)(1) Sec 1.4(a)  
223 (b)(1) Sec 1.4(a)  
224  
225  
226  
227  
228  
229  
230  
231  
232

233  
234 (a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
235 issues and systems (b)(1) Sec 1.4(a)  
236 (b)(1) Sec 1.4(a)  
237

238  
239 (b) (~~S//REL USA, AUS, GBR~~) Reference the GIG (b)(1) Sec 1.4(a)  
240 (b)(1) Sec 1.4(a)  
241

242  
243 (2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
244 (b)(1) Sec 1.4(a) Report any changes in or events that cause changes to:

245  
246 (a) (U) USSTRATCOM mission, availability of USSTRATCOM forces or  
247 unexpected loss of a USSTRATCOM asset.

# SECRET

157 (2) (U) USSTRATCOM will recommend that (b)(1) Sec 1.7(e) conduct Joint Staff  
158 Integrated Vulnerability Assessments (JSIVA), with or without a DCIP module,  
159 or Balanced Survivability Assessments (BSA) via USNORTHCOM, for CONUS  
160 based assets, other Geographic COCOMs for OCONUS based assets, and the  
161 Joint Staff. These assessments will complete gaps in information or validate  
162 dated information.

163  
164 (3) (U) USSTRATCOM will request additional resources to support  
165 solutions outlined in all of USSTRATCOM's remediation plans and future  
166 characterization efforts.

## 167 168 4. (U) Administration and Logistics

169  
170 a. (U) Administration. Refer to Base Plan.

171  
172 b. (U) Logistics

173  
174 (1) (U) Refer to Base Plan.

175  
176 (2) (U) The Services and Agencies are responsible for funding subordinate  
177 unit CIP programs. Commanders have the inherent responsibility to  
178 implement prudent CIP measures and will immediately elevate any identified  
179 CIP concerns to their next higher headquarters or responsible command.  
180 Commanders may provide additional support through advocacy and/or  
181 funding of critical CIP issues.

## 182 183 5. (U) Command and Control

184  
185 a. (U) Command

186  
187 (1) (U) Command Relationships.

188  
189 (2) (U) Command Posts. Refer to Base Plan.

190  
191 b. (U) Command, Control, Communications, and Computer (C4) Systems.  
192 See Annex K.

193  
194 c. (U) Reporting Requirements

195  
196 (1) (U) Refer to Base Plan.

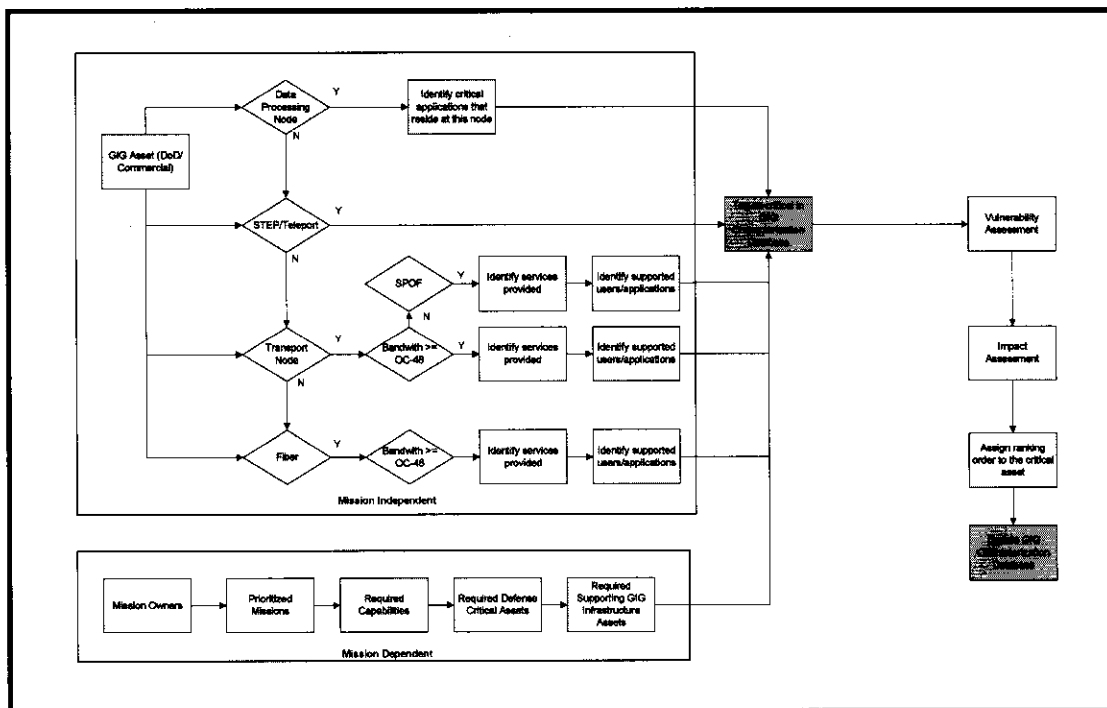
197  
198 (2) (U) All units and Commanders must immediately report any incident,  
199 threat, surveillance or suspicious activity that may adversely impact  
200 infrastructure supporting USSTRATCOM operational capability.

201

SECRET

C-16-6

Figure C-16-3: The GIG Characterization Methodology (U)



134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

(2) (U) DOD Components asset owners will remediate vulnerabilities to their critical assets/infrastructure. Remediation includes actions taken to correct known deficiencies and weaknesses once vulnerabilities have been identified. The JTF GNO will make recommendations to the CC/S/As in support of their risk management efforts. The asset owner's remediation plans will include recommendations to either accept the risk, or remediate the risk via a Doctrine-Organization- Training-Material-Leadership-Personnel-Facilities (DOTMLPF) approach. The factors to be considered are as follows:

(a) (U) Assess the ability to use material vs. non-material solutions to include alternative funding solutions if necessary.

(b) (U) Incorporate CIP into Exercise Plans.

(c) (U) Provide lessons learned to improve the GIG risk management processes.

c. (U) Coordinating Instructions

(1) (U) USSTRATCOM will coordinate (b)(1) Sec 1.7(e) to assist in the Characterization of the GIG. See Figure 2.



**SECRET**

110 ranked based on their impact to the performance of the GIG. (b)(1) Sec 1.7(e)  
111 (b)(1) Sec 1.7(e)  
112  
113

<u>DEFENSE SECTOR</u>	<u>LEAD AGENCY</u>
Defense Industrial Base (DIB)	Defense Contract Management Agency (DCMA)
Financial Services	Defense Finance and Accounting Services (DFAS)
Global Information Grid (GIG)	(b)(1) Sec 1.7(e)
Health Affairs	Assistant Secretary of Defense (ASD) for Health Affairs (HA)
Intelligence, Surveillance, and Reconnaissance (ISR)	(b)(1) Sec 1.7(e)
Logistics	Defense Logistics Agency (DLA)
Personnel	DOD Human Resources Activity (DHRA)
Public Works	U.S. Army Corps of Engineers (USACE)
Space	USSTRATCOM
Transportation	United States Transportation Command (USTRANSCOM)

114

115

Figure C-16-2: DCIP Defense Sector Lead Agencies (U)

117

118 (7) (U) Priorities. USSTRATCOM CIP protection priorities are based on  
119 critical C4 missions in support of the NMS. GIG mission success will depend  
120 upon accurately characterizing the GIG, Identifying critical GIG assets,  
121 determining vulnerabilities, and mitigating risk.

122

b. (U) Tasks

123

124

(1) (U) (b)(1) Sec 1.7(e)

125

(b)(1) Sec 1.7(e)

126

127 responsibility of characterizing the GIG. See Figure 3 below. This  
128 characterization process will clearly define inter/intra dependencies of DOD  
129 and non-DOD assets, single points of failure, and commercial dependencies in  
130 support of the NMS. All validated GIG task critical assets approved by the joint  
131 staff will be added to the GIG Geospatial Database that's presently maintained  
132 by the (b)(1) Sec 1.7(e) Mission Assurance Division.

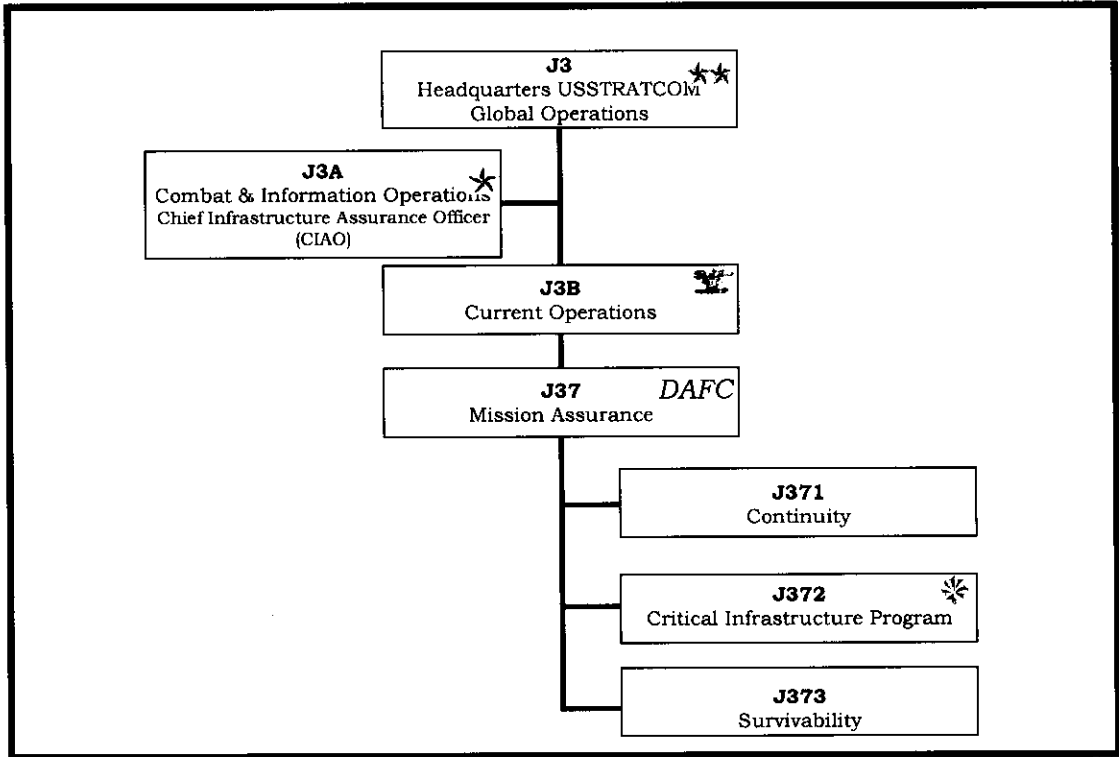
**SECRET**

**SECRET**

86 (5) (U) Monitoring and Reporting (M&R). The M&R process is not solely

87 (b)(1) Sec 1.7(e)

92 Figure 1 below. The endstate is to integrate CIP into existing command reporting processes.



95 Figure C-16-1: USSTRATCOM CIP Organizational Structure (U)

96 (U) The USSTRATCOM's Mission Assurance Division (J37), is the office  
97 of primary responsibility to establish, resource, and execute the command's  
98 program for matters pertaining to the identification of Defense Infrastructures  
99 and the prioritization/protection of Defense *Critical* Infrastructure, including  
100 the identification and prioritization of USSTRATCOM mission essential tasks  
101 and required capabilities.

102 (6) (U) Criticality. The GIG critical assets are identified from both  
103 mission dependent and mission independent perspective. Mission-dependent  
104 critical assets are those deemed essential to the accomplishment of a mission.  
105 Their identification and prioritization are top down driven i.e. from mission to  
106 supporting infrastructure. Mission-independent critical assets are derived and  
107  
108  
109

**SECRET**

41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85

c. (U) Friendly: See Annex A (Task Organization). There are no friendly forces specifically assigned to protect the critical infrastructure of the United States. Rather, CIP is a national effort to establish, resource, and execute a process for matters pertaining to the identification of Defense Infrastructures and the prioritization/protection of Defense *Critical* Infrastructures. In this effort, it is important to understand that CIP and Force Protection (FP) are complementary efforts. USSTRATCOM's JTF\_GNO will rely on the following organizations to enhance the success of its delegated USSTRATCOM mission to direct the operations and defense of the GIG:

- (1) (U) (b)(1) Sec 1.7(e)
- (2) (U) (b)(1) Sec 1.7(e)
- (3) (U) (b)(1) Sec 1.7(a)
- (4) (U) Counterintelligence Field Agency (CIFA)
- (5) (U) Law Enforcement/Counterintelligence (LE/CI) Agency

d. (U) Assumptions. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution. The execution of CIP remains the same throughout the (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

a. (U) Concept of Operations

(1) (U) Commander's Intent. CDRUSSTRATCOM intends to prevent or mitigate the loss or degradation of task critical assets that support assigned global missions.

(2) (U) Purpose. Identify, prioritize, and recommend protection measures to defend critical GIG assets.

(3) (U) Methods. Accurately characterize the GIG, and establish a standardized criticality methodology, and a real time situation awareness capability that will accurately support the identification of critical GIG assets.

(4) (U) Endstate. Focus scarce resources on the most critical vulnerabilities, and integrate CIP into operational planning processes.

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AFB NE 68113-6500  
28 February 2008

1  
2 APPENDIX 16 TO ANNEX C TO STRATCOM CONPLAN 8039 (U)

3 (U) OPR: JTF-GNO, J5

4 GIG CRITICAL INFRASTRUCTURE PROTECTION (CIP) Execution Plan (U)

5  
6 (U) References:

7  
8 a. (U) Homeland Security Presidential Directive (HSPD) 7, Critical  
9 Infrastructure Identification, Prioritization, and Protection, 17 Dec 03

10  
11 b. (U) DODD 3020.40, Defense Critical Infrastructure Program (DCIP), 19  
12 Aug 05

13  
14 c. (U) DODD 3020.40, Defense Critical Infrastructure Program (DCIP), Apr  
15 07 Draft

16  
17 d. (U) Strategic Command Directive (SD) 536-1, Critical Infrastructure  
18 Program, 15 Jul 05

19  
20 e. (U) Joint Concept of Operations for Global Information Grid NetOps, 4  
21 Aug 06

22  
23 f. (U) DCIP Security Classification Guide, March 2007 Draft Version 2.1

24  
25 1. (U) Situation

26  
27 a. (U) Background: DODD 3020.40 provides policy, and assigns  
28 responsibilities for the DCIP. DCIP was conceived at the National level as a  
29 risk management strategy to provide processes, tools, and methodologies for  
30 making economic choices about what type of protection will be employed for  
31 critical infrastructure assets to assure their continued availability. DCIP  
32 requires an understanding of mission impact to guide the prioritization of  
33 enterprise-wide protection efforts; vulnerability remediation investment  
34 strategies; operational and procedural enhancement; and contingency plan  
35 development. Protection derives from reducing or eliminating vulnerabilities.  
36 This Annex will focus on critical GIG cyber assets IAW USSTRATCOMs UCP  
37 mission which encompasses directing GIG operations and defense capabilities.

38  
39 b. (U) (b)(1) Sec 1.7(e) See Annexes B (Intelligence) (b)(1) Sec 1.7(e)

~~Classified by: Multiple Sources~~

~~Reason: 1.4(a), (e), and (g)~~

~~Declassify on: 26 February 2032~~

40 (b)(1) Sec 1.7(e)

**SECRET**

C-16-1

**SECRET**

313 simulation process itself will be used as a tool to visualize how the  
314 Operations/Campaign may flow. Additionally, modeling and simulation will be  
315 used to support analysis of collection opportunities, as well as offering COCOM  
316 staffs an opportunity to evaluate the plan for shortfalls, gaps and other  
317 complications that may not have been observed in previous collection planning  
318 efforts.

319

320 c. (U) Tasks

321

322 (1) ~~(S//REL)~~ JFCC ISR will (b)(1) Sec 1.4(a)

323

(b)(1) Sec 1.4(a) in support of

324

CONPLAN 8039.

325

326

327

(2) ~~(S//REL USA, AUS, GBR)~~ JFCC GSI will coordinate and integrate  
operations in and through cyberspace with JFCC NW, JTF GNO, JIOWC, and as  
required with JFCC Space (b)(1) Sec 1.4(a)

328

329

(b)(1) Sec 1.4(a)

330

331

d. (U) Coordinating Instructions. Refer to the Base Plan.

332

333

4. (U) Administration and Logistics. Refer to the Base Plan.

334

335

5. (U) Command and Control. Refer to the Base Plan.

SECRET

267 allocation (b)(1) Sec 1.4(a)  
268 (b)(1) Sec 1.4(a) capabilities.

269  
270 (4) (U) Operations Center. JFCC ISR maintains 24/7 ISR Operations Center  
271 for situational awareness of global ISR operations. JFCC ISR's watch will monitor  
272 all (b)(1) Sec 1.7(e)

273 (b)(1) Sec 1.7(e)  
274  
275  
276  
277  
278  
279  
280

281  
282 (5) (U) (b)(1) Sec 1.7(e)

283 (b)(1) Sec 1.7(e)  
284  
285  
286

287  
288 (6) (U) Portal. The current JFCC ISR portal serves as a hub for ISR  
289 information sharing within the DOD. The information accessible within this portal  
290 consists of a collection of pages for publishing JFCC ISR specific content and  
291 multiple links to resources external to the portal. The version 2 of JFCC ISR web-  
292 based portal will be capable of supporting internal and external coordination and  
293 collaboration. The JFCC ISR Portal will be critical resource for DOD's ISR  
294 community and a vital enabler of the JFCC ISR mission.

295  
296 (7) (U) Assessment

297  
298 (a) (U) Assessing Collection. JFCC ISR will develop criteria for assessing  
299 collection mechanisms in order to determine the effectiveness of synchronization,  
300 resolution of tasking, asset competition, and customer satisfaction. JFCC ISR  
301 Assessment Division will, in coordination with the JFCCs, Services, IC, CSA, and  
302 COCOMs, develop, maintain, use and evaluate measures of effectiveness and  
303 mission metrics to assess ISR mission objective accomplishment. JFCC ISR will  
304 use USSTRATCOM, JFCC GSI, JFCC NW, JTF GNO, JIOWC, and combatant  
305 command inputs and planning factors as a baseline, conducting assessment  
306 process will be captures and used to inform subsequent planning and allocation  
307 efforts.

308  
309 (b) (U) Modeling and Simulation Methodologies. After reviewing the plan,  
310 JFCC ISR Assessments Division will use COCOM inputs to initiate Modeling and  
311 Simulation (MOD/SIM) to support analysis of specific ISR Operations/Campaigns.  
312 While JFCC ISR will develop specialized MOD/SIM tools, the modeling and

SECRET

222 4. (U) Re-allocate. This involves moving an asset/capability assigned  
223 against an existing requirement to the newly identified requirement. This re-  
224 allocation can be from within the requesting GCC's AOR, or from another AOR.  
225

226 5. (U) Surge. This involves a specified time-frame during which  
227 selected assets/capabilities will be surged to meet the requirement.  
228

229 6. (U) Utilize ISR (b)(1) Sec 1.7(e) to meet the  
230 requirement.  
231

232 7. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
233 recommended allocation changes.  
234

235 8. (~~S//REL USA, AUS, GBR~~) JFCC ISR will develop (b)(1) Sec 1.4(a)  
236 (b)(1) Sec 1.4(a)  
237 allocation recommendation based on asset availability for specific requirement.  
238

239 9. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) consolidate the  
240 recommendation (b)(1) Sec 1.4(a)  
241 (b)(1) Sec 1.4(a) will make the final decision and assets will be allocated  
242 accordingly.  
243

244 (3) (U) Support for Operations in and Through Cyberspace  
245

246 (a) (~~S//REL USA, AUS, GBR~~) Operations in and through cyberspace have  
247 unique requirements in the electromagnetic spectrum. (b)(1) Sec 1.4(a)  
248 (b)(1) Sec 1.4(a)

249  
250 (b)(1) Sec 1.4(a) In this case, JFCC ISR will coordinate  
251 with JFCC NW to satisfy (b)(1) Sec 1.4(a) JFCC  
252 ISR will leverage DOD ISR (b)(1) Sec 1.4(a)  
253 right capabilities to go against the identified collection requirements.  
254

255 (b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) JFCC  
256 ISR's flexible ISR options, if and when (b)(1) Sec 1.4(a)  
257 (b)(1) Sec 1.4(a) support of operations in and through  
258 cyberspace.  
259

260 (c) (U) JFCC ISR (b)(1) Sec 1.7(e)  
261 (b)(1) Sec 1.7(e)  
262  
263

264 (d) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
265 (b)(1) Sec 1.4(a)  
266 JFCC ISR will provide (b)(1) Sec 1.4(a) recommendations if the current ISR

SECRET

176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221

2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

3. (~~S//REL USA, AUS, GBR~~) In a (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

4. (~~S//REL USA, AUS, GBR~~) The (b)(1) Sec 1.4(a)  
continue to be improved to provide (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) timely fashion. Request for

additional ISR support, (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) requires additional coordination.

(d) (~~S//REL USA, AUS, GBR~~) Re-allocation. JFCC ISR will (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

1. (U) National Intelligence Priority.

2. (U) GCCs/USSTRATCOM (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

3. (U) Risk (associated with not gaining the information).

4. (U) Potential value of intelligence to be gathered.

(e) (U) COAs. JFCC ISR will develop potential COAs for consideration. A list of factors will be provided with each COA to facilitate decision making. Those COAs include:

1. (U) Coordination with the CC/S/As to determine if the requirement is being, or can be, met via any existing ISR operations.

2. (~~S//REL USA, AUS, GBR~~) If at all possible, (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

3. (U) Allocate. This means to allocate an asset/capability that is not currently assigned against the requirement.



130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175

(b)(1) Sec 1.4(a)

cyberspace operations forces and capabilities. Also, as required, JFCC ISR will develop and maintain a

(b)(1) Sec 1.4(a)

appropriate entities to access. JFCC ISR is responsible for providing all ISR partners with global situational awareness of ISR activities.

(2) (U) ISR Force Management Concepts. JFCC ISR established

(b)(1) Sec 1.7(e)

reallocation and COAs recommendations will provide the flexibility to modify existing allocation plan to better meet combatant command requirements in a timely manner.

(a) (FOUO)

(b)(1) Sec 1.7(e)

(b) (FOUO)

(b)(1) Sec 1.7(e)

1. (FOUO) Requirements for this ISR

(b)(1) Sec 1.7(e)

2. (FOUO) While supporting Geographic Combatant Commander ISR requirements, these forces enable USSTRATCOM to integrate ISR in support of strategic and global operations.

(c) (~~S//REL USA, AUS, GBR~~) If an immediate requirement is identified for additional ISR support

(b)(1) Sec 1.4(a)

1. (~~S//REL USA, AUS, GBR~~) The

(b)(1) Sec 1.4(a)

SECRET

(b)(1) Sec 1.7(e)

representation within JFCC ISR.

(U)(3) (~~S//REL USA, AUS, GBR~~) USSTRATCOM, JFCCs and Centers. JFCC ISR will closely coordinate with USSTRATCOM, JFCC GSI and JFCC NW to support CONPLAN 8039. JFCC ISR will coordinate with other USSTRATCOM component commands to meet the CONPLAN 8039 objectives. In this effort, JFCC ISR will participate through collaborative sessions facilitated by USSTRATCOM, JFCC GSI, or other JFCCs, combatant command(s) and recommend ISR COAs if required.

(4) (U) (b)(1) Sec 1.7(e) JFCC ISR will work in conjunction with the

(b)(1) Sec 1.7(e)

CONPLAN 8039.

(5) (U) Services. The Service representatives within JFCC ISR serve as the primary conduit/liasion into their respective Service for coordinating ISR issues. Coordination between JFCC ISR and JFCOM and its components will be done to address issues (b)(1) Sec 1.7(e) processes, and determination of availability and capability of Service-specific ISR assets. Additionally, each Service will receive process and disseminate data via their respective and existing ISR processes and procedures.

(6) (U) Allies and PN. To the maximum extent possible, PN ISR capabilities will be utilized when available and appropriate. (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

b. (U) Mission Execution

(1) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) JFCC ISR will coordinate with USSTRATCOM (b)(1) Sec 1.4(a) ISR (b)(1) Sec 1.4(a) JFCC ISR will monitor these operations and be prepared to assist the Unified Commanders in modifying the operation to ensure mission success. Concerning cyberspace, JFCC ISR will (b)(1) Sec 1.4(a)

SECRET

SECRET

38 networked systems and associated physical infrastructures. (b)(1) Sec 1.4(a)  
39 (b)(1) Sec 1.4(a)  
40

41 (b) (~~S//REL USA, AUS, GBR~~) Other on-going activities (i.e., Global War on  
42 Terrorism (GWOT), Contingency Operations) (b)(1) Sec 1.4(a)  
43 (b)(1) Sec 1.4(a)  
44

45 (c) (~~S//REL USA, AUS, GBR~~) Other collection capabilities may be  
46 leveraged on a case-by-case basis. There may be opportunities (b)(1) Sec 1.4(a)  
47 (b)(1) Sec 1.4(a)  
48  
49

50 (2) (U) Constraints. None Identified.

51  
52 2. (U) Mission. Refer to the Base Plan.

53  
54 3. (U) Execution

55  
56 a. (~~S//REL USA, AUS, GBR~~) Concept of Operations. ISR operations include  
57 those processes carried out (b)(1) Sec 1.4(a)  
58 (b)(1) Sec 1.4(a)  
59  
60

61 (b)(1) Sec 1.4(a) The role of JFCC ISR is not to provide the analytical research  
62 of collected data, but recommend the resources to adequately respond to critical  
63 needs in the form of sensors, platforms and specific processing suites. While  
64 integrating all intelligence disciplines, JFCC ISR will ensure its focus also includes  
65 (b)(1) Sec 1.4(a)  
66  
67  
68  
69  
70  
71

72 (1) (~~S//REL USA, AUS, GBR~~) General. JFCC ISR will coordinate and seek  
73 (b)(1) Sec 1.4(a)  
74  
75  
76  
77  
78

79 (2) (U) Organization and Mission Partners. JFCC ISR is a component  
80 (b)(1) Sec 1.7(e)  
81  
82  
83

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
28 February 2008

APPENDIX 9 TO ANNEX C TO USSTRATCOM CONPLAN 8039 (U)

(U) OPR: JFCC ISR

INTELLIGENCE SURVEILLANCE AND RECONNAISSANCE (ISR) (U)

(U) References:

a. (U) Draft Horizontal Command and Control Integration (HC2I), Apr 2007 (S)

b. (U) Draft Joint Functional Component Command (JFCC) ISR Concept of Operations (CONOPS), 21 Aug 06 (FOUO)

1. (U) Situation

a. (U) General

(1) (~~S//REL USA, AUS, GBR~~) The strategic goal of CONPLAN 8039 is to ensure US military freedom of action in cyberspace and to deny adversary freedom of action in cyberspace. To achieve this goal, (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

when directed.

b. (U) (b)(1) Sec 1.7(e) Refer to Annex B (Intelligence) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

c. (U) Friendly. Refer to Annex A (Task Organization) and the Base Plan.

d. (U) Assumptions. Refer to the Base Plan.

e. (U) Limitations

(1) (U) Restraints

(a) (~~S//REL USA, AUS, GBR~~) Cyberspace is a domain using electronics

~~Classified by: Multiple Sources~~

~~Reason: 1.4(a), (e), and (g)~~

~~Declassify on: 26 February 2032~~

and the electromagnetic spectrum to store, modify, and exchange data via

**SECRET**

C-9-1

**SECRET**

(INTENTIONALLY BLANK)

**SECRET**

C-8-4

**SECRET**

87 commanders may use any lawful weapon or tactic available for mission  
88 accomplishment.

89  
90 (3) (U) (b)(1) Sec 1.7(e) During ROE development, careful consideration must be  
91 given to (b)(1) Sec 1.7(e) anticipated  
92 operations. The ROE development cell will need to identify what actions are  
93 subject to specific ROE (e.g. reference a, Enclosure F, Paragraph 3.b.) and  
94 whether any supplemental ROE will be required (b)(1) Sec 1.7(e)

95  
96 (4) (U) Self-defense. As described in reference a, unit commanders  
97 always retain the inherent right and obligation to exercise unit self-defense in  
98 response to a hostile act or demonstrated hostile intent. Unit commanders  
99 may limit individual self-defense by members of their unit. Both unit and  
100 individual self-defense includes defense of other US Military forces in the  
101 vicinity. The hostile act standard described in Enclosure A of reference a, does  
102 not apply to a subset of digital protection options under this plan, (b)(1) Sec 1.7(e)  
103 (b)(1) Sec 1.7(e) Refer to Enclosure F of reference a.

104  
105  
106 b. (U) Tasks – Required Legal Reviews. It is the responsibility of the legal  
107 staffs to confirm that required legal reviews for a capability/weapon to be  
108 utilized in a cyberspace operation have been completed, as well as to do any  
109 operational legal reviews. It is the responsibility of the operators to ensure that  
110 a legal review is conducted for proposed operations.

111  
112 c. (U) Coordinating Instructions. As stated above, coordination may need to  
113 take place with the Interagency and non-US forces. In addition, Enclosure F of  
114 reference a, reference b, and other DOD instructions and policies require

115 (b)(1) Sec 1.7(e)  
116

117  
118 4. (U) Administration. Refer to Base Plan.

119  
120 5. (U) Command and Control. It is possible that USSTRATCOM may be the  
121 supported commander, supporting commander, or a combination of both  
122 depending on the particular activities to be undertaken. In any of these cases,  
123 USSTRATCOM planners, operators, and attorneys must ensure that  
124 appropriate ROE are developed to carry out the missions assigned.

125

# SECRET

41 (SROE), but also theater ROE, existing EXORDs, and DOD authorities such as  
42 the (b)(1) Sec 1.4(a)

43  
44 b. (U) Scope/Applicability. This appendix applies to all US forces and  
45 personnel conducting missions pursuant to this plan.

46  
47 c. (U) (b)(1) Sec 1.7(e) Refer to Base Plan, Annex B, (b)(1) Sec 1.7(e)

48  
49 d. (U) Friendly. Refer to Base Plan. Although not subject to ROE, there  
50 may be significant involvement between US forces and the Interagency to  
51 achieve overall US objectives. In some operations, non-US forces may  
52 participate in cyberspace operations under this plan. ROE for non-US forces  
53 may differ from the ROE issued to US forces. In such cases, coordination and  
54 deconfliction with the non-US force will need to take place unless classification,  
55 OPSEC, or operational considerations prevent such coordination.

56  
57 e. (U) Assumptions. Refer to Base Plan.

58  
59 f. (U) Legal Considerations. All operations under this plan will be  
60 conducted in compliance with US law and the law of war. Per reference b,  
61 members of the DOD Components will comply with the law of war during all  
62 armed conflicts, however such conflicts are characterized, and in all other  
63 military operations. For the legal considerations applicable to intelligence  
64 collection refer to Annex B, Intelligence.

65  
66 g. (U) Concept. ROE are a means of providing guidance and instruction  
67 to military commanders and DOD components within the framework of overall  
68 political directives and the law of war. They define the degree and manner in  
69 which force may be applied and are designed to ensure its carefully controlled  
70 application in order to achieve specified objectives. Additionally, they ensure  
71 the maximum survivability of USSTRATCOM and other forces in a  
72 confrontation with adversary forces.

73  
74 2. (U) Mission. Refer to Base Plan.

75  
76 3. (U) Execution

77  
78 a. (U) Concept of Operation

79  
80 (1) (U) General. CJCS Standing ROE contained in reference a, serve  
81 as the starting point for development of ROE for an operation.

82  
83 (2) (U) Lawful tactics / weapons. The SROE, reference a, are designed  
84 to be permissive in nature. Therefore, unless a specific weapon or tactic  
85 requires SecDef or combatant commander approval, or unless a specific  
86 weapon or tactic is restricted by an approved supplemental measure,

SECRET

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
28 February 2008

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40

APPENDIX 8 TO ANNEX C TO USSTRATCOM CONPLAN 8039 (U)

(U) OPR: USSTRATCOM HQ SJA  
RULES OF ENGAGEMENT (ROE) (U)

(U) References:

a. (U) CJCSI 3121.01B, Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces, 13 Jun 05 (S)

b. (U) DOD 2311.01E, DOD Law of War Program, 9 May 06 (U)

c. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)  
Activities, 9 May 07 (S//NF)

1. (U) Situation

a. (~~S//REL USA, AUS, GBR~~) Purpose. The purpose of this appendix is to address rules for conducting cyberspace operations. Given that the scope and nature of contemplated operations under CONPLAN 8039 are quite diverse, this appendix contains a discussion of the issues that will need to be addressed in the ROE for a specific operation. Supplemental ROE will almost certainly have to be requested from SECDEF in order to carry out operations under this CONPLAN. As stated in the Base Plan, (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) The ROE for an operation will need to enable the supported Combatant Commander and supporting Combatant Commanders to carry out cyberspace operations, including

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) Authorization to carry out specific parts of an operation may depend on (b)(1) Sec 1.4(a) the

(b)(1) Sec 1.4(a)

operations). IO in particular tend to require higher level authorizations. The planners, operators, and attorneys who work together to develop appropriate

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (c), and (g)~~  
~~Declassify on: 26 February 2032~~

ROE will need to look not only at ref a, the Standing Rules of Engagement



**SECRET**

(INTENTIONALLY BLANK)

**SECRET**  
C-3-G-4

# SECRET

86 (a) (U) (b)(1) Sec 1.7(e) operations are planned and executed IAW  
87 SECDEF SROE for Information Operations and the USSTRATCOM (b)(1) Sec 1.7(e)  
88 (b)(1) Sec 1.7(e)

- 89
- 90 4. (U) Administration and Logistics. Refer to the Base Plan.
- 91
- 92 5. (U) Command and Control. Refer to the Base Plan.

SECRET

C-3-G-3

SECRET

40 (b)(1) Sec 1.4(a) based on the situation.

41  
42 (2) (~~S//REL TO USA, AUS, CAN, GBR, NZL~~) (b)(1) Sec 1.4(a)  
43 commander or head of major DOD component is the approving authority for  
44 the employment of (b)(1) Sec 1.4(a)

45 (b)(1) Sec 1.4(a)  
46  
47  
48  
49

50 should report response actions and results to the JTF GNO as this input is  
51 critical to other response actions that may be necessary and GIG situational  
52 awareness in general. (b)(1) Sec 1.4(a)

53 (b)(1) Sec 1.4(a)  
54

55  
56 (a) (~~S//REL TO USA, AUS, CAN, GBR, NZL~~) (b)(1) Sec 1.4(a)  
57 (b)(1) Sec 1.4(a)  
58

59  
60 (b) (~~S//REL TO USA, AUS, CAN, GBR, NZL~~) (b)(1) Sec 1.4(a) System  
61 Description (b)(1) Sec 1.4(a)

62  
63 (c) (~~S//REL TO USA, AUS, CAN, GBR, NZL~~) (b)(1) Sec 1.4(a)  
64 (b)(1) Sec 1.4(a)

65  
66 (d) (~~S//REL TO USA, AUS, CAN, GBR, NZL~~) Significant results (b)(1) Sec 1.4(a)  
67 (b)(1) Sec 1.4(a)

68  
69 (e) (~~S//REL TO USA, AUS, CAN, GBR, NZL~~) (b)(1) Sec 1.4(a)  
70 (b)(1) Sec 1.4(a)

71  
72 (3) (~~S//REL TO USA, AUS, CAN, GBR, NZL~~) (b)(1) Sec 1.4(a) The CDR  
73 USSTRATCOM is the approving authority for the employment of RA techniques  
74 (b)(1) Sec 1.4(a)  
75  
76 (b)(1) Sec 1.4(a) CC/S/A. Combatant Commands or  
77 Service component NetOps HQ request (b)(1) Sec 1.4(a) from  
78 the CDR USSTRATCOM via JTF GNO.  
79

80  
81 (4) (~~S//REL TO USA, AUS, CAN, GBR, NZL~~) (b)(1) Sec 1.4(a) The  
82 Commander, USSTRATCOM is the approving authority for (b)(1) Sec 1.4(a)  
83 (b)(1) Sec 1.4(a)  
84  
85

SECRET

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
28 February 2008

TAB G TO APPENDIX 3 TO ANNEX C TO CONPLAN 8039 (U)

(U) OPR: JTF-GNO J5  
RESPONSE ACTIONS (U)

(U) References. Refer to the Base Plan.

1. (U) Situation. Refer to the Base Plan. The purpose of this is to articulate definitions, boundaries and responsibilities for Response Actions (RA) in defense of the GIG.

2. (U) Mission. Refer to the Base Plan.

3. (U) Execution

a. (U) Concept of Operations. For the purpose of this plan, RAs are deliberate, authorized measures, or activities that protect and defend DOD computer systems and networks under attack or targeted for attack by adversary computer systems/networks. RAs extend DOD's layered defense-in-depth capabilities and increase DOD's ability to withstand adversary attacks. RAs consist of techniques and administrative procedures employed to halt or minimize the effects of malicious activity and/or intrusion. RAs comprise the entire set of defensive actions to protect and defend the DOD GIG. (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

b (U) Specific Guidance for RAs

(1) (~~S//REL TO USA, AUS, CAN, GBR, NZL~~) (b)(1) Sec 1.4(a)  
commander is the approving authority for the employment of response actions

(b)(1) Sec 1.4(a)

This reporting is critical to the overall defense of the GIG and situational awareness in general. CC/S/A's advise and coordinate as necessary on (b)(1) Sec 1.4(a)

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (c), and (g)~~  
~~Declassify on: 26 February 2032~~

**SECRET**

224

225

226

227

228

229

230

231

232

233

234

235

INTENTIONALLY BLANK

**SECRET**

C-3-F-6

SECRET

178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223

(b)(1) Sec 1.4(a)

(a) (~~S//REL USA, AUS, GBR~~) Be prepared to support (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) to Appendix 3 (Information Operations) and Annex Y (Strategic Communication).

(b) (U) (b)(1) Sec 1.7(e) employed forces.

(c) (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) US vital interests.

(d) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) data or the medium used to transmit or store the data.

(2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

b. (U) Tasks. Refer to the (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

c. (U) Coordinating Instructions. Refer to the (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) and CONPLAN 8035.

4 (U) Administration and Logistics. Refer to the (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

5 (U) Command and Control

a. (U) Command Relationships

(1) (U) Roles and Responsibilities. Refer to Annex J (Command Relationships) and the Base Plan. Refer also to (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) If forces are delegated OPCON/TACON to USSTRATCOM, USSTRATCOM will further delegate TACON to JFCC NW.

(2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Communication and Reporting Requirements. The (b)(1) Sec 1.4(a) is used for coordinating all (b)(1) Sec 1.4(a) portions of this plan. Refer to (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

**SECRET**

132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177

(b)(1) Sec 1.4(a)

(a) (U) (b)(1) Sec 1.7(e)  
threatening US vital interests.

(b) (~~S~~//REL USA, AUS, GBR) Support (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) to Appendix 3 (Information Operations) and  
Annex Y (Strategic Communication).

(c) (U) (b)(1) Sec 1.7(e)

(d) (U) (b)(1) Sec 1.7(e)

(e) (~~S~~//REL USA, AUS, GBR) Support Operational (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) to Appendix 3 (Information  
Operations).

(f) (U) Maintain the capability to support deterrence/follow-on  
operations against other potential adversaries.

4. (~~S~~//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

**SECRET**

86 considered. Refer to (b)(1) Sec 1.7(e) to Appendix 3  
87 (Information Operations) and Annex Y (Strategic Communication).

88  
89 2. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

90 (b)(1) Sec 1.4(a)

91  
92 (b)(1) Sec 1.4(a)

93 USSTRATCOM will lead  
94 a collaborative effort across the USSTRATCOM Staff, Functional Components,  
95 Service Components, combatant commanders, Joint Staff, and a Joint

96 (b)(1) Sec 1.4(a)

97  
98  
99  
100  
101  
102  
103  
104  
105 (a) (U) (b)(1) Sec 1.7(e)

106 (b)(1) Sec 1.7(e)

107  
108 (b) (U) (b)(1) Sec 1.7(e)

109  
110 (c) (S//REL USA, AUS, GBR) Support (b)(1) Sec 1.4(a)

111 (b)(1) Sec 1.4(a)

112 (b)(1) Sec 1.4(a) to Appendix 3 (Information Operations) and  
113 Annex Y (Strategic Communication).

114  
115 (d) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

116 (b)(1) Sec 1.4(a)

117  
118 (e) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

119 (b)(1) Sec 1.4(a)

120  
121  
122 (f) (S//REL USA, AUS, GBR) Support Operational (b)(1) Sec 1.4(a)

123 (b)(1) Sec 1.4(a)

124 to Appendix 3 (Information  
125 Operations).

126 3. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

127 (b)(1) Sec 1.4(a)

128  
129  
130  
131  
**SECRET**

C-3-F-3



SECRET

40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85

(1) (~~S//REL USA, AUS, GBR~~) USSTRATCOM will (b)(1) Sec 1.4(a) LAW references (a) through (e) above, Plan Summary, and Base Plan.

(a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) operations, USSTRATCOM will (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

1. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(a) (U) Identify threats to US interests and assess (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(b) (U) (b)(1) Sec 1.7(e)

interagency partners, allies, and GCCs. Identify (b)(1) Sec 1.7(e) in support of plan activities that will (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(c) (U) Establish force posture and conditions tailored to (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(d) (U) Use of (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) will be

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
28 February 2008

1 TAB F TO APPENDIX 3 TO ANNEX C TO USSTRATCOM CONPLAN 8039 (U)

2 (U) OPR: JFCC NW

3 (b)(1) Sec 1.7(e) (U)

5 (U) References: Refer to the Base Plan.

7 a. (U) (b)(1) Sec 1.7(e)

8 (b)(1) Sec 1.7(e) United States Strategic  
9 Command (USSTRATCOM) and Delegation of Authority," 14 Aug 2003 (S//NF)

11 b. (U) (b)(1) Sec 1.7(e)

12 (b)(1) Sec 1.7(e)  
13 Headquarters Commands to USSTRATCOM," 1 Oct 2003 (S//NF)

15 c. (U) (b)(1) Sec 1.7(e)

16 (b)(1) Sec 1.7(e) Jan 2004 (With Modifications 1, 2, and 3)

17 (U)

19 d. (U) SECDEF Memorandum, Subject: "Appointment of the Commander,  
20 JFCC NW," 12 Jul 2005 (S)

22 e. (U) USSTRATCOM Operational Order (OPORD) 07-01, 1 Nov 2006

24 1. (U) Situation

26 a. (U) (b)(1) Sec 1.7(e) Refer to Annex B (Intelligence) (b)(1) Sec 1.7(e)

27 (b)(1) Sec 1.7(e)

29 b. (U) Friendly. Refer to Annex A (Task Organization), the Base Plan and

30 (b)(1) Sec 1.7(e)

32 c. (U) Assumptions. Refer to the Base Plan (b)(1) Sec 1.7(e)

33 (b)(1) Sec 1.7(e)

35 2. (U) Mission. Refer to the Base Plan.

37 3 (U) Execution

39 a. (U) Concept of Operations

Classified by: Multiple Sources  
Reason: 1.4(a), (c), and (g)  
Declassify on: 26 February 2032

**SECRET**

C-3-F-1

**SECRET**

131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146

b. (~~S//REL USA, AUS, GBR~~) Coordinating Instructions. Planners should compare and evaluate the merit of (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) Refer to the Base Plan for an example of a (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

will be deconflicted by USSTRATCOM.

4. (U) Administration and Logistics. Refer to the Base Plan.

5. (U) Command and Control. Refer to the Base Plan, Annex J (Command Relationships).

SECRET

85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130

(b)(1) Sec 1.4(a)

(4). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) through cyberspace  
can be used to (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(5). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) Consider the  
activities below as representative activities that may be best achieved through

(b)(1) Sec 1.4(a)

(a). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b.) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) through the cyberspace domain.

(c). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) through  
the cyberspace domain.

(d). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(e). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(f). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) USSC

(g). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(h). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(i). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

SECRET

**SECRET**

39 the mission space for command and control of forces; some use the internet to  
40 conduct recruiting and develop the financial support that is the lifeblood of  
41 modern terrorism, others use it as a means to subvert regimes and  
42 governments; others use it in active, opposing "fire fights," i.e., combat in  
43 cyberspace to deny freedom of action to the US.

44  
45 c. (U) Assumptions. Refer to the Base Plan.

46  
47 2. (U) Mission. Refer to the Base Plan.

48  
49 3. (U) Execution. Refer to the Base Plan.

50  
51 a. (U) Concept of Operations

52  
53 (1). (U) Purpose

54  
55 (a). (U) The purpose of this Tab is to provide a common level of  
56 understanding of the requirement to (b)(1) Sec 1.7(e)  
57 planning operations in and through cyberspace.

58  
59 (b). (U) Additionally, this Tab illustrates (b)(1) Sec 1.7(e)  
60 that can be integrated into operations in and through cyberspace and generate  
61 an effect in the cyberspace domain. (b)(1) Sec 1.7(e)

62 (b)(1) Sec 1.7(e)

63  
64 (2). (~~S//REL USA, AUS, GBR~~) General. (b)(1) Sec 1.4(a)

65 (b)(1) Sec 1.4(a)

66 cyberspace operations.

67 Availability of (b)(1) Sec 1.4(a) within cyberspace affords a combatant

68 commander a wide variety of (b)(1) Sec 1.4(a) that can

69 (b)(1) Sec 1.4(a)

70  
71  
72  
73  
74  
75  
76  
77  
78 (3). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

79 (b)(1) Sec 1.4(a)

**SECRET**

C-3-E-2

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
28 February 2008

1 TAB E TO ANNEX C TO USSTRATCOM CONPLAN 8039 (U)

2 (U) OPR: JFCC NW J52

3 (b)(1) Sec 1.7(e) (U)

4  
5 (U) References: Refer to the Base Plan and Appendix 3 (Information  
6 Operations) to Annex C (Operations).

7  
8 1. (U) Situation. Refer to the Base Plan.

9  
10 a. (U//~~FOUO~~) General. Our Adversaries are using cyberspace to execute  
11 command and control, to enhance logistics and acquisition, to disseminate  
12 their ideology of violence, solicit and gather the finances for operations, train  
13 the present cadre of insurgents in traditional and modern TTPs, and radicalize  
14 the next generation of terrorists. One way to effectively disrupt their freedom of  
15 maneuver in these efforts is by (b)(1) Sec 1.7(e)

16 (b)(1) Sec 1.7(e)

17  
18  
19  
20  
21  
22 (1). (U//~~FOUO~~) For the purpose of this document, (b)(1) Sec 1.7(e)

23 (b)(1) Sec 1.7(e)

24  
25 actions that affect adversary information.

26  
27 (2). (U//~~FOUO~~) Opportunities to neutralize, counter, or prosecute  
28 adversary operations in and through cyberspace will emerge and disappear  
29 within minutes, at best, and seconds, at worst. While (b)(1) Sec 1.7(e)

30 (b)(1) Sec 1.7(e)

31  
32  
33 b. (U//~~FOUO~~) Adversary. (b)(1) Sec 1.7(e)

34 (b)(1) Sec 1.7(e)

35 (adversaries) targeting the USG with multiple objectives,  
36 operating at different levels of competence and capability, in struggles of  
37 differing philosophies and ends – all occurring simultaneously. Some  
38 adversaries are content to intrude on and exfiltrate data in mass; others use

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (c), and (g)~~  
~~Declassify on: 26 February 2032~~

**SECRET**

C-3-E-1

~~SECRET~~

(INTENTIONALLY BLANK)

~~SECRET~~  
C-3-D-4

**SECRET**

83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110

c. (U) Coordinating Instructions

(1) (S//REL) (b)(1) Sec 1.4(a) Respective  
combatant command (b)(1) Sec 1.4(a)  
When required, (b)(1) Sec 1.4(a)

(2) (S//REL) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(3) (U) USSTRATCOM Component Commands will integrate planning efforts to achieve CDRUSSTRATCOM and combatant command objectives and desired effects.

(4) (S//REL) CDRUSSTRATCOM will coordinate with combatant commanders in order to develop, and provide to those commands, IO capabilities that can be used to achieve objectives (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

4. (U) Administrative and Logistics. Refer to the Base Plan.

5. (U) Command and Control. Refer to the Base Plan and Annex J (Command Relationships).



**SECRET**

41 planning and employment with all affected COCOMs and DOD Components.

42

43 (b). (S//REL) Coordinate (b)(1) Sec 1.4(a)

44 (b)(1) Sec 1.4(a) with affected Combatant Commands, DOD Components,

45 (b)(1) Sec 1.4(a)

46

47

48 (c). (S//REL) Coordinate with all applicable (b)(1) Sec 1.4(a)

49 (b)(1) Sec 1.4(a)

50

51 (d). (S//REL) USSTRATCOM components and supported COCOMs will

52 (b)(1) Sec 1.4(a)

53

54

55 (e). (S//REL) USSTRATCOM (b)(1) Sec 1.4(a)

56 (b)(1) Sec 1.4(a)

57

58

59 (f). (S//REL) USSTRATCOM and subordinate Joint Combatant  
60 Commands/JTFs will coordinate necessary action for supported Combatant  
61 Commands/Services/Agencies (CC/S/A) (b)(1) Sec 1.4(a)

62 (b)(1) Sec 1.4(a)

63

64 (2) (U) Combatant Commands

65

66 (a). (S//REL) Coordinate (b)(1) Sec 1.4(a) ISR resources

67 (b)(1) Sec 1.4(a) and USSTRATCOM as required.

68

69 (b). (S//REL) Coordinate (b)(1) Sec 1.4(a)

70 (b)(1) Sec 1.4(a) surveillance assets as required in accordance with all

71 applicable (b)(1) Sec 1.4(a)

72

73 (c). (S//REL) Develop and/or manage the (b)(1) Sec 1.4(a)

74 (b)(1) Sec 1.4(a)

75

76 (d). (C//REL) Maintain, update, and provide access to the combatant

77 command (b)(1) Sec 1.4(a)

78

79 (e). (S//REL) Conduct (b)(1) Sec 1.4(a) surveillance to

80 help ensure freedom of action in cyberspace to USG. (b)(1) Sec 1.4(a)

81 (b)(1) Sec 1.4(a)

82

**SECRET**

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NEBRASKA 68113-6500  
28 February 2008

TAB D TO APPENDEX C TO USSTRATCOM CONPLAN 8039 (U)

(U) OPR: JIOWC

(b)(1) Sec 1.7(e) (U)

(U) References: Refer to Base Plan.

a. (U) (b)(1) Sec 1.7(e) 31 Jul 2002 (S)

b. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) Feb 1996 (U)

c. (U) (b)(1) Sec 1.7(e) 7 Apr 2000 (U)

d. (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) 1 Oct 1993 (FOUO)

1. (U) Situation. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution

a. (~~S//REL~~) Concept of Operations. For the purpose of CONPLAN 8039,

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) These and Intelligence, Surveillance,  
and Reconnaissance (ISR) assets conduct operations globally to ensure freedom  
of action in cyberspace for the US, (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) IAW

applicable combatant command standing rules of engagement (ROE).

b. (U) Tasks

(1) (U) USSTRATCOM

(a). (~~S//REL~~) Coordinate (b)(1) Sec 1.4(a)

~~Classified by: Multiple Sources~~

~~Reason: 1.4(a), (c), and (g)~~

~~Declassify on: 26 February 2032~~

# SECRET

222 (2) (U//~~FOUO~~) A strict "need-to-know" policy must be announced,  
223 enforced, and maintained throughout the entire operation. The need-to-know  
224 policy should cover classified and unclassified information. While all personnel  
225 must be familiar with the critical information list, personnel do not have a  
226 need-to-know specific facts comprising critical information for areas of the plan  
227 in which they are not involved. Limiting information distribution will  
228 dramatically reduce the chances for accidental compromise of unclassified, but  
229 sensitive information that is critical to the success of the operation.

230  
231 (3) (U//~~FOUO~~) Initiation and termination of OPSEC measures and  
232 related activities will be coordinated through the OPSEC Working Group.

233  
234 (4) (U//~~FOUO~~) Dissemination of the critical information list as widely as  
235 possible within security and OPSEC guidelines is essential to OPSEC  
236 awareness.

237  
238 (5) (U//~~FOUO~~) Provisions of OPSEC support to this plan should be  
239 coordinated with the PAO (b)(1) Sec 1.7(e)

240  
241 (6) (U) OPSEC Concerns. Personnel are encouraged to contact the  
242 USSTRATCOM OPSEC Officer to report OPSEC concerns, request guidance,  
243 and to provide suggestions for process improvement.

## 244 245 4. (U) Administration and Logistics

246  
247 a. (U) Administration. Command OPSEC program officers/managers must  
248 be appointed in writing. Identify in writing these OPSEC officers/managers to  
249 the STRATCOM J39/JFCC GSI J39 OPSEC officer.

250  
251 b. (U) Logistics. Not used.

## 252 253 5. (U) Command and Control

254  
255 a. (U) OWG. An OWG comprised of representatives from all supporting  
256 Combatant Commands/Joint Force Commands supporting this plan will be  
257 convened as necessary. Reporting of OPSEC disclosures to the OWG will be  
258 made for the purpose of ensuring the currency of OPSEC awareness as it  
259 pertains to this plan.

260  
261 b. (U) OPSEC Procedures. Conduct periodic reviews and evaluations of  
262 OPSEC procedures in order to improve the USSTRATCOM OPSEC Program.

263

SECRET

C-3-C-6

~~SECRET~~

177 (b) (U//~~FOUO~~) In coordination with J6, update monitoring priorities  
178 and key word lists.

179  
180 (c) (U//~~FOUO~~) Attend all planning group meetings / discussions to  
181 include (b)(1) Sec 1.7(e)

182  
183 (2) (U//~~FOUO~~) J2

184  
185 (a) (U//~~FOUO~~) Provide an assessment of the effectiveness of OPSEC  
186 countermeasures.

187  
188 (b) (~~S//REL USA, AUS, GBR~~) Utilize the OPSEC process to enable  
189 other (b)(1) Sec 1.4(a)

190 (b)(1) Sec 1.4(a)

191  
192 (3) (~~C~~) J6

193  
194 (a) (U//~~FOUO~~) Identify secure/encrypted communications shortfalls  
195 based upon CONPLAN operations.

196  
197 (b) (~~C//REL USA, AUS, GBR~~) Develop a communications plan that  
198 (b)(1) Sec 1.4(a)

199  
200  
201 (4) (U//~~FOUO~~) PAO. Coordinate PA Guidance with OPSEC Working  
202 Group in order to prevent disclosures.

203  
204 (5) (~~C//REL USA, AUS, GBR~~) Force Protection. Coordinate facility  
205 (b)(1) Sec 1.4(a)

206  
207  
208 (6) (U//~~FOUO~~) Division Chiefs (or OWG members). Periodically remind  
209 staff personnel of USSTRATCOM critical information and indicators,  
210 vulnerabilities, and adversary intelligence collection capabilities.

211  
212 c. (U) Coordinating Instructions

213  
214 (1) (U//~~FOUO~~) To protect against collection from adversaries,  
215 USSTRATCOM personnel must be cognizant when using unsecured means of  
216 communications such as the NIPRNET, facsimile, cell phones, Defense  
217 Switching Network (DSN) telephones, and common telephones. Anytime  
218 personnel are communicating over an unsecure or unencrypted means of  
219 communication they must not disclose critical or sensitive information  
220 pertaining to CONPLAN 8039.

221

# SECRET

133                   5. (U) Details of military ties, agreements, arrangements between  
134 the DOD, the interagency, commercial industries, and partner nations.  
135

136                   6. (U) Details of security measures or procedures with other  
137 federal, state, or local agencies. Vulnerabilities, discovered through regular  
138 cyberspace assessments, and those corrective measures recommended.  
139

140                   7. (U) Capabilities, facility and network diagrams, infrastructure  
141 layouts, connectivity information, status/readiness of cyberspace assets, alert  
142 status/procedures of forces supporting this CONPLAN.  
143

144                   8. (U) Details and vulnerabilities of a Combatant Commander's  
145 C4ISR architecture and physical security infrastructure.  
146

147                   9. (U) Operational and technical details, including Tactics,  
148 Techniques, and Procedures (TTP), of cyberspace operations.  
149

150           d. (U) Assumptions. Refer to Base Plan.  
151

152           2. (U) Mission. Refer to Base Plan.  
153

154           3. (U) Execution

155           a. (U) Concept of Operations. The purpose of OPSEC is to prevent  
156 adversaries from obtaining friendly critical information. While OPSEC should  
157 be practiced at the same rigor whether in garrison, during training, or deployed  
158 conducting operations, leaders at all levels are encouraged to remind their  
159 personnel of the importance of OPSEC during the planning and execution of  
160 this CONPLAN and to apply OPSEC TTPs to protect critical information and  
161 indicators regarding force intentions, capabilities, and vulnerabilities. The  
162 OPSEC process will be integrated into this plan, and its supporting plans and  
163 operations, to the fullest extent possible. Based on identification of critical  
164 information, analysis of the threat and friendly vulnerabilities, OPSEC  
165 officers/managers/planners will assess risk to mission and then implement  
166 appropriate countermeasures to increase overall mission effectiveness.  
167

168           b. (U) Tasks

169                   (1) (U//~~FOUO~~) USSTRATCOM OPSEC Officer

170                   (a) (U//~~FOUO~~) Use the OPSEC Working Group (OWG) meeting to  
171 evaluate CILs and countermeasures and promulgate the OPSEC plan. The  
172 OWG members will then increase OPSEC awareness within their respective  
173 directorate to decrease the chance of critical information disclosure.  
174  
175  
176

# SECRET

C-3-C-4

# SECRET

87  
88 (d) (U) Assess Risk. A determination of how much damage to the  
89 cyberspace mission and commander's intent will be caused by the  
90 loss/disclosure of the critical information.  
91

92 (e) (U) Implement Countermeasures. Anything that effectively negates  
93 an adversary's ability to gather or exploit friendly critical information or that  
94 renders the possession of the critical information useless. While not a formal  
95 step of the OPSEC Process, (b)(1) Sec 1.7(e)  
96 (b)(1) Sec 1.7(e) the OPSEC planner to monitor utility of implemented  
97 countermeasures and, if required, re-initiate the cyclic nature of the OPSEC  
98 process to improve on the actions taken.  
99

## 100 (3) (U) Critical Information

101  
102 (a) (U) In any operation, it is vital to achieve 'essential secrecy' which  
103 is the condition achieved as a result of denying adversaries friendly forces  
104 critical information. Because of the requirements to share operational  
105 information across many agencies and to other governments, care must be  
106 taken to emphasize the need to protect critical information.  
107

108 (b) (U) Critical Information is the specific facts about friendly  
109 intentions, capabilities, and activities vitally needed by adversaries for them to  
110 plan and act effectively so as to cause a delay, disruption, total failure, or  
111 unacceptable consequences for friendly mission accomplishment.  
112

113 (c) (U) Each C/S/A supporting this plan will develop a Critical  
114 Information List (CIL). Once developed, the CIL will be used to support the 5-  
115 step OPSEC process. The following are generalized Critical Information items  
116 that pertain to this CONPLAN. Actual words and/or phrases that address or  
117 provide specifics covered below must not be discussed over non-secure means  
118 or in public spaces in order to protect critical information from disclosure and  
119 adversary exploitation.  
120

121 1. (U) Association of the operational execution of this CONPLAN  
122 with any specific target or country.  
123

124 2. (U) Association of this CONPLAN with exercises, operational  
125 rehearsals, or other mission-specific training that supports this CONPLAN.  
126

127 3. (U) Association of abbreviations, acronyms, nicknames, or code  
128 words with this CONPLAN or locations.  
129

130 4. (U) Movement/billeting of forces and senior decision makers  
131 when conducted in support of this plan.  
132

SECRET

C-3-C-3

# SECRET

41 (3) (U) Responsibility for OPSEC. OPSEC is a command responsibility.  
42 At each level of command, the operations officer (or equivalent), has staff  
43 responsibility for coordinating overall OPSEC planning. Every individual  
44 involved with or supporting CONPLAN 8039 must assist in safeguarding  
45 classified and unclassified information deemed sensitive or critical to the  
46 success of this CONPLAN.

47  
48 b. (U) (b)(1) Sec 1.7(e)

49 (b)(1) Sec 1.7(e)

50  
51 c. (U) Friendly Forces. Refer to Base Plan and Annex A (Task Organization).

52  
53 (1) (U) Friendly Operations. Adversaries can exploit OPSEC vulnerabilities  
54 and correlate information obtained by various collection and exploitation  
55 methods. Therefore, we must operate in such a manner as to deny friendly  
56 information necessary for adversaries to accurately estimate the military  
57 situation/friendly capability, and simultaneously contribute to adversely  
58 affecting their decision cycles.

59  
60 (2) The OPSEC process. OPSEC is a continuous analytical process which  
61 focuses on identifying, controlling, and protecting evidence associated with any  
62 operation. OPSEC is not a physical, personnel, or information security system;  
63 nor is it a collection of rules or instructions. Like the overall integration of IO,  
64 OPSEC is a function of planning; this planning must apply appropriate  
65 countermeasures to achieve desired effects during execution of operations.  
66 IAW reference (b), all Combatant Commands and supporting joint forces will  
67 use the five-step OPSEC process:

68  
69 (a) (U) Identify Critical Information. That information, if exploited by  
70 an adversary, would significantly impede friendly operations or prevent mission  
71 accomplishment. Combatant Commands should provide their critical  
72 information lists to USSTRATCOM and other pertinent Combatant Commands,  
73 to facilitate protection of sensitive information.

74  
75 (b) (U) Analyze the Threat. A formal assessment of the adversary's  
76 capability and intent to exploit any critical information. Combatant  
77 Commands should task supporting intelligence elements to provide analysis  
78 tailored for OPSEC planners that focus on cyberspace threats and as  
79 appropriate, state and non-state threat collection capabilities and intentions.

80 (b)(1) Sec 1.7(e) related  
81 information that must be considered by personnel when planning for,  
82 exercising, or conducting cyberspace operations.

83  
84 (c) (U) Analyze Vulnerabilities (and specific signatures / indicators). A  
85 determination of how susceptible cyberspace operations related critical  
86 information is to loss/disclosure.

# SECRET

C-3-C-2

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AFB, NE 68113-6500  
28 February 2008

TAB C TO APPENDIX 3 TO ANNEX C TO US STRATEGIC COMMAND CONPLAN  
8039 (U)

(U) OPR: JIOWC/J36  
OPERATIONS SECURITY (U)

(U) References. Refer to Base Plan and Appendix 3 (Information Operations) to Annex C (Operations).

a. (U) CJCSI 3213.01B, Joint Operations Security, 17 Dec 2003 (U)

b. (U) Joint Pub 3-13.3, Joint Doctrine for Operations Security, 29 Jun 2006 (U)

c. (U) CJCSI 6510.01D, Information Assurance and Computer Network Defense, 15 Jun 2004 (U)

1. (U) Situation. Refer to Base Plan.

a. (U) General

(1) ~~(S//REL USA, AUS, GBR)~~ Purpose. This Tab provides planning guidance for integrating OPSEC into CONPLAN 8039

(b)(1) Sec 1.4(a)

(2) (U) Overview. OPSEC is the process of denying adversaries information about friendly intentions and capabilities by identifying, controlling, and protecting indicators associated with planning and conducting of operations and other activities. When applied, OPSEC measures prevent an adversary's timely exploitation of critical friendly information relating to operational plans, special technologies, capabilities, and relationships. OPSEC measures include protection of primarily unclassified information that can model or profile friendly intentions and capabilities through analysis, compilation, and integration of multiple-source information including that available through open sources and international media coverage.

~~Classified by: Multiple Sources  
Reason: 1.4(a), (c), and (g)  
Declassify on: 26 February 2032~~



**SECRET**

PAGE INTENTIONALLY BLANK

**SECRET**  
C-3-B-2

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
28 February 2008

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36

TAB B TO APPENDIX 3 TO ANNEX C TO USSTRATCOM CONPLAN 8039 (U)

(U) OPR: HQ USSTRATCOM J39

(b)(1) Sec 1.7(e) (U)

(U) References: Refer to the Base Plan.

1. (U) Situation. Refer to the Base Plan.

2. (U) Mission. Refer to the Base Plan.

3. (~~S//REL USA, AUS, GBR~~) Execution. Information concerning (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) in CONPLAN 8039 is handled in (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) is required.

4. (U) Administration and Logistics. Refer to the Base Plan.

5. (U) Command and Control. Refer to the Base Plan.

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (c), and (g)~~  
~~Declassify on: 26 February 2032~~

**SECRET**

C-3-B-1

**SECRET**

570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589

INTENTIONALLY BLANK

**SECRET**

C-3-A-14

**SECRET**

541 5. (~~S//REL USA, AUS, GBR~~) Command and Control. CDRUSSTRATCOM is  
542 the supported commander for planning and may be designated the supported  
543 commander for execution. As required, (b)(1) Sec 1.4(a) will provide the  
544 supported commander the necessary (b)(1) Sec 1.4(a)

545 (b)(1) Sec 1.4(a) The supported commander will identify  
546 (b)(1) Sec 1.4(a)  
547  
548  
549

550  
551 a. (~~S//REL USA, AUS, GBR~~) Headquarters Locations and movements. As  
552 required, (b)(1) Sec 1.4(a)

553 (b)(1) Sec 1.4(a)  
554  
555

556  
557 b. (~~S//REL USA, AUS, GBR~~) Supporting (b)(1) Sec 1.4(a)

558 (b)(1) Sec 1.4(a)  
559

560  
561 c. (U) C4 support requirements and responsibilities for (b)(1) Sec 1.7(e)  
562 liaison officers are situation dependent based on (b)(1) Sec 1.7(e)

563 (b)(1) Sec 1.7(e)  
564  
565  
566  
567

568 computer networks.  
569

SECRET

495 (g) (S//REL USA, AUS, GBR) Confirm capabilities and (b)(1) Sec 1.4(a)

496 (b)(1) Sec 1.4(a)  
497  
498  
499

500 (h) (S//REL USA, AUS, GBR) As required, assist in the identification  
501 and staffing of (b)(1) Sec 1.4(a)

502 (b)(1) Sec 1.4(a)  
503  
504  
505  
506

507 (4) (U) (b)(1) Sec 1.7(e)  
508 when requested.

509  
510 4. (U) Administration and Logistics. The requirements below reflect those  
511 necessary for sustainment in the event (b)(1) Sec 1.7(e)

512 (b)(1) Sec 1.7(e) supported commander.

513  
514 a. (U) Administration. Not used.

515  
516 b. (U) Logistics

517  
518 (1) (U) ICW USSTRATCOM, and (b)(1) Sec 1.7(e) the affected GCC will

519 (b)(1) Sec 1.7(e)  
520  
521  
522  
523  
524 requirements.

525  
526 (2) (U) USSTRATCOM ICW (b)(1) Sec 1.7(e) and the affected GCC will  
527 coordinate the (b)(1) Sec 1.7(e) equipment and  
528 materials.

529  
530 (3) (U) USSTRATCOM ICW (b)(1) Sec 1.7(e) and the affected GCC will  
531 coordinate fiscal matters relating to special funds.

532  
533 (4) (U) USSTRATCOM ICW (b)(1) Sec 1.7(e) and the affected GCC will  
534 coordinate (b)(1) Sec 1.7(e)

535  
536 (5) (U) USSTRATCOM will coordinate movement of personnel and  
537 equipment to (b)(1) Sec 1.7(e)

538 (b)(1) Sec 1.7(e)  
539  
540

SECRET

449 (e) (U) Coordinate (b)(1) Sec 1.7(e)

450

451 (2) (U) (b)(1) Sec 1.7(e)

452

453 (a) (S//REL USA, AUS, GBR) Plan, develop, coordinate, (b)(1) Sec 1.4(a)

454 (b)(1) Sec 1.4(a)

455

456

457

458 (b) (b) (S//REL USA, AUS, GBR) ICW affected GCCs, request support  
459 from (b)(1) Sec 1.4(a) as required.

460

461 (c) (S//REL USA, AUS, GBR) Coordinate (b)(1) Sec 1.4(a)

462 (b)(1) Sec 1.4(a) with GCCs.

463

464 (d) (S//REL USA, AUS, GBR) ICW (b)(1) Sec 1.4(a) and the affected GCC,

465 (b)(1) Sec 1.4(a)

466

467

468 (e) (S//REL USA, AUS, GBR) Coordinate with (b)(1) Sec 1.4(a) affected

469 GCCs, (b)(1) Sec 1.4(a)

470 (b)(1) Sec 1.4(a)

471

472

473

474 (3) (U) Commander (b)(1) Sec 1.7(e)

475

476 (a) (S//REL USA, AUS, GBR) Prepare (b)(1) Sec 1.4(a) in  
477 support of cyberspace operations.

478

479 (b) (S//REL USA, AUS, GBR) Conduct (b)(1) Sec 1.4(a)

480 (b)(1) Sec 1.4(a)

481

482 (c) (S//REL USA, AUS, GBR) Conduct (b)(1) Sec 1.4(a)

483

484 (d) (S//REL USA, AUS, GBR) Provide copies of all cyberspace related  
485 products to (b)(1) Sec 1.4(a) and affected GCCs.

486

487 (e) (S//REL USA, AUS, GBR) Determine critical requirements

488 shortfalls (b)(1) Sec 1.4(a)

489 (b)(1) Sec 1.4(a)

490

491

492 (f) (S//REL USA, AUS, GBR) Develop and provide detailed (b)(1) Sec 1.4(a)

493 (b)(1) Sec 1.4(a)

494

SECRET

**SECRET**

403 conventional missions and units as necessary. Commander, (b)(1) Sec 1.4(a)  
404 (b)(1) Sec 1.4(a)  
405  
406

407 (d) (~~S//REL USA, AUS, GBR~~) CDRUSSTRATCOM/Geographic  
408 Combatant Commanders. Be prepared to (b)(1) Sec 1.4(a)  
409 (b)(1) Sec 1.4(a) as requested and required.

410  
411 (3) (U) Authorities

412  
413 (a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Geographic Combatant  
414 Commander's are the approval authority (b)(1) Sec 1.4(a)  
415 (b)(1) Sec 1.4(a)  
416

417  
418 (b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
419 (b)(1) Sec 1.4(a)

420  
421 (c) (~~S//REL USA, AUS, GBR~~) The designated supported commander  
422 for execution is delegated (b)(1) Sec 1.4(a)  
423 (b)(1) Sec 1.4(a)

424  
425 (d) (~~S//REL USA, AUS, GBR~~) Geographic Combatant Commanders.  
426 In coordination with (b)(1) Sec 1.4(a)  
427 (b)(1) Sec 1.4(a)  
428  
429  
430  
431

432  
433 e. (U) Tasks

434  
435 (1) (U) GCCs

436  
437 (a) (~~S//REL USA, AUS, GBR~~) Integrate cyberspace (b)(1) Sec 1.4(a)  
438 (b)(1) Sec 1.4(a)

439  
440 (b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
441 (b)(1) Sec 1.4(a) cyberspace operations strategy.

442  
443 (c) (U) Accept OPCON or TACON (b)(1) Sec 1.7(e) to conduct  
444 operations.

445  
446 (d) (U) Be prepared to provide Service-unique capability to support  
447 (b)(1) Sec 1.7(e)  
448

SECRET

358  
359 4 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

360 (b)(1) Sec 1.4(a)

361  
362 (f) (U) USG National Goal 6: Defending US citizens and interests at  
363 home and abroad.

364  
365 1 (U) (b)(1) Sec 1.7(e)

366  
367 2 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

368 (b)(1) Sec 1.4(a)

369  
370  
371 b. (U) End State. Refer to the Base Plan.

372  
373 c. (U) Situation Monitoring and Measures of Effectiveness. Intelligence  
374 (b)(1) Sec 1.7(e) security monitoring, and operational  
375 feedback mechanisms to support this CONPLAN and determine measures of  
376 effectiveness will be determined for each situation, permissive or otherwise.

377  
378 d. (U) Control

379  
380 (1) (S//REL USA, AUS, GBR) Approval Process. The (b)(1) Sec 1.4(a)

381 (b)(1) Sec 1.4(a) and  
382 cyberspace (b)(1) Sec 1.4(a) USSTRATCOM thru coordination with

383 the (b)(1) Sec 1.4(a) USSTRATCOM  
384 recommends cyberspace (b)(1) Sec 1.4(a)

385 submits cyberspace (b)(1) Sec 1.4(a) for

386 approval. Once cyberspace (b)(1) Sec 1.4(a) are approved CDRUSSTRATCOM  
387 is the (b)(1) Sec 1.4(a)

388 (b)(1) Sec 1.4(a)  
389 (b)(1) Sec 1.4(a) In all other cases, the GCC is delegated product approval authority.

390  
391 (2) (U) Responsibilities

392  
393 (a) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) guidance  
394 and programs approval authority.

395  
396 (b) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

397 (b)(1) Sec 1.4(a) approval and dissemination authority to the designated  
398 Supported Commander (b)(1) Sec 1.4(a)

399 (b)(1) Sec 1.4(a)

400  
401 (c) (S//REL USA, AUS, GBR) Commander, (b)(1) Sec 1.4(a)

402 (b)(1) Sec 1.4(a)



312

313

3 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

314

(b)(1) Sec 1.4(a)

315

316

(c) (U) USG National Goal 3: Defeat terrorist organizations.

317

318

1 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

319

(b)(1) Sec 1.4(a)

320

321

2 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

322

(b)(1) Sec 1.4(a)

323

324

325

3 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

326

(b)(1) Sec 1.4(a)

327

328

4 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

329

(b)(1) Sec 1.4(a)

330

331

(d) (U) USG National Goal 4: Deny sponsorship/support/sanctuary to terrorist organizations.

332

333

334

1 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

335

(b)(1) Sec 1.4(a)

336

337

2 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

338

(b)(1) Sec 1.4(a)

339

340

341

3 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

342

(b)(1) Sec 1.4(a)

343

344

345

4 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

346

(b)(1) Sec 1.4(a)

347

348

(e) (U) USG National Goal 5: Diminish the underlying causes of terrorism.

349

350

351

1 (U) (b)(1) Sec 1.7(e)

352

353

2 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

354

(b)(1) Sec 1.4(a)

355

356

3 (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

357

(b)(1) Sec 1.4(a)

SECRET

266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311

2. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

3. (S//REL USA, AUS, GBR) US (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

4. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

5. (S//REL USA, AUS, GBR) The victims (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b) (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(d) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

most significant (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

The

(6) (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(a) (U) USG National Goal 1: Deter aggression and counter coercion.

1 (U) (b)(1) Sec 1.7(e)

2 (U) (b)(1) Sec 1.7(e)

community.

(b) (U) USG National Goal 2: Dissuade/Defeat potential adversaries.

1 (U) (b)(1) Sec 1.7(e)

2 (U) (b)(1) Sec 1.7(e)

**SECRET**

223 (2) (~~S//REL USA, AUS, GBR~~) Guidance. CDRUSSTRATCOM thru  
224 coordination with (b)(1) Sec 1.4(a)  
225 (b)(1) Sec 1.4(a)  
226  
227

228 activities. Initiate required actions to deploy forces required in support of  
229 USSTRATCOM CONPLAN 8039.

230  
231 (3) (U) (b)(1) Sec 1.7(e) will be  
232 developed and included in the appropriate appendices to (b)(1) Sec 1.7(e)  
233 (b)(1) Sec 1.7(e)

234  
235 (4) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
236 CDRUSSTRATCOM thru coordination with CDRUSSOCOM will develop and  
237 publish in (b)(1) Sec 1.4(a)  
238 (b)(1) Sec 1.4(a)

239  
240 (5) (U) (b)(1) Sec 1.7(e)  
241

242 (~~S//REL USA, AUS, GBR~~) Operational Guidance. OPE will be used to provide  
243 predictive analysis (b)(1) Sec 1.4(a)

244 (b)(1) Sec 1.4(a)  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257

258 (a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
259 (b)(1) Sec 1.4(a)  
260  
261

262  
263 1. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
264 (b)(1) Sec 1.4(a) to those  
265 goals.

179 (b)(1) Sec 1.4(a)

180  
181 (5) (S) Use (b)(1) Sec 1.4(a)

182 (b)(1) Sec 1.4(a)

183  
184 g. (U) Assumptions. Refer to the Base Plan.

185  
186 (1) (S) Interagency information (b)(1) Sec 1.4(a)

187 (b)(1) Sec 1.4(a)

188  
189 (2) (S) (b)(1) Sec 1.4(a)

190 (b)(1) Sec 1.4(a)

191  
192  
193 2. (U) Mission. Refer to the Base Plan.

194 3. (U) Execution

195  
196 a. (U) Concept of Operations. The purpose of (b)(1) Sec 1.7(e)

197 (b)(1) Sec 1.7(e)

212 (1) (~~S~~//REL USA, AUS, GBR) Overview. Advise the CJCS,  
213 USSTRATCOM, and GCCs on cyberspace information measures, themes, and

214 (b)(1) Sec 1.4(a)

**SECRET**

133 (k) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

134 (b)(1) Sec 1.4(a)

136 (l) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

138 (b)(1) Sec 1.4(a)

140 (m) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

141 (b)(1) Sec 1.4(a)

143 (n) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

144 (b)(1) Sec 1.4(a)

149 (o) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

150 (b)(1) Sec 1.4(a)

154 (p) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

155 (b)(1) Sec 1.4(a)

159 (4) (U) Command Systems. Refer to Annex B (Intelligence) (b)(1) Sec 1.7(e)

160 (b)(1) Sec 1.7(e)

162 e. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

163 (b)(1) Sec 1.4(a)

166 f. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) Tasks

168 (1) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

169 (b)(1) Sec 1.4(a)

171 (2) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

172 (b)(1) Sec 1.4(a) decision-making process.

174 (3) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

175 (b)(1) Sec 1.4(a)

178 (4) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

SECRET

88  
89 (2) (U) (b)(1) Sec 1.7(e) US military  
90 operations ISO this plan.

91  
92 d. (U) (b)(1) Sec 1.7(e) Refer to the Base Plan, Annex B  
93 (Intelligence), (b)(1) Sec 1.7(e)

94  
95 (1) (U) Decision Maker and Staff. Refer to Annex B (Intelligence) and  
96 (b)(1) Sec 1.7(e)

97  
98 (2) (U) Intelligence Systems. Refer to Annex B (Intelligence) (b)(1) Sec 1.7(e)  
99 (b)(1) Sec 1.7(e)

100  
101 (3) (U) Target Audiences

102  
103 (a) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
104 (b)(1) Sec 1.4(a)

105  
106 (b) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
107 (b)(1) Sec 1.4(a)

108  
109 (c) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
110 (b)(1) Sec 1.4(a)

111  
112 (d) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

113  
114 (e) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

115  
116 (f) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

117  
118 (g) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) theater of  
119 operations.

120  
121 (h) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
122 (b)(1) Sec 1.4(a)

123  
124  
125 (i) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
126 (b)(1) Sec 1.4(a) operations in and through  
127 cyberspace within their jurisdiction.

128  
129 (j) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
130 (b)(1) Sec 1.4(a)  
131  
132

**SECRET**

42 1. (U) Situation

43  
44 a. (~~S//REL USA, AUS, GBR~~) Overview.

45 Cyberspace can play a role in the conduct (b)(1) Sec 1.4(a)  
46 (b)(1) Sec 1.4(a) via the Global  
47 Information Grid (GIG). (b)(1) Sec 1.4(a) is responsible for the  
48 development and approval (b)(1) Sec 1.4(a) the cyberspace  
49 community can support as one of many methods (b)(1) Sec 1.4(a)  
50 (b)(1) Sec 1.4(a)  
51

52  
53 b. (U) US and Allied Perspective

54  
55 (1) (U) Refer to the Base Plan and Annex A (Task Organization).

56  
57 (2) (U) US Department of State (DOS)

58  
59 (a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
60 (b)(1) Sec 1.4(a)  
61  
62

63 prior to the initiation of cyberspace activities.

64  
65 (b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Furnishes  
66 advice (b)(1) Sec 1.4(a)  
67 (b)(1) Sec 1.4(a)  
68 communications capabilities. The Office may release select (b)(1) Sec 1.4(a)  
69 assets to the appropriate combatant command's control IAW (b)(1) Sec 1.4(a)  
70 (b)(1) Sec 1.4(a)

71  
72 (3) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
73 (b)(1) Sec 1.4(a)  
74  
75

76 (4) (~~S//REL USA, AUS, GBR~~) Under Secretary of Defense - Policy (USD-P)  
77 . Will delegate (b)(1) Sec 1.4(a)  
78 CDRUSSTRATCOM upon request and implementation of CONPLAN 8039.

79  
80 (5) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
81 (b)(1) Sec 1.4(a) US agencies per  
82 existing agreements.

83  
84 c. (U) Neutral Perspective

85  
86 (1) (U) Refer to the Base Plan, Annex B (Intelligence), (b)(1) Sec 1.7(e)  
87 (b)(1) Sec 1.7(e)

SECRET

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AFB, NE 68113-6500  
28 February 2008

TAB A TO APPENDIX 3 TO ANNEX C TO USSTRATCOM CONPLAN 8039 (U)  
(U) OPR: JIOWC/J36

(b)(1) Sec 1.7(e) (U)

(U) References. Refer to the Base Plan.

a. (U) Executive Order 12333, 4 December 1981, "United States Intelligence Activities"

b. (U) (b)(1) Sec 1.7(e)

c. (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) (S)

d. (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) (FY) 2002."

e. (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

FY 2002."

f. (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

g. (U) Joint Pub 3-57.1, 14 April 2003, "Joint Doctrine for Civil Affairs."

h. (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

i. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (c), and (g)~~  
~~Declassify on: 26 February 2032~~

SECRET

C-3-A-1



**SECRET**

677 (b)(1) Sec 1.4(a)

678 Operations.

679

680 c. (~~S//REL USA, AUS, GBR~~) Determination of command relationships  
681 (TACON / OPCON) of forces shall be provided in published

682 WARNORD(S)/EXORD(S) or the applicable (b)(1) Sec 1.4(a)

683 (b)(1) Sec 1.4(a)

684

685 d. (U) External Agency Support. During exercises and contingencies,  
686 USSTRATCOM components and agencies such as, but not limited to JIOWC,  
687 JFCC NW, JTF\_GNO, DISA, the JWAC, and Joint COMSEC Monitoring Agency,  
688 may deploy to USSTRATCOM AOR or a supporting location as required.

689

690

691 Tabs:

692 A - (U) (b)(1) Sec 1.7(e)

693 B - (U) Electronic Warfare

694 C - (U) Operations Security

695 D - (U) (b)(1) Sec 1.7(e)

696 E - (U)

697 F - (U)

698 G - (U) Response Actions

**SECRET**

631 4. (~~S//REL USA, AUS, GBR~~) USSTRATCOM. Develop and conduct

632 (b)(1) Sec 1.4(a)  
633  
634

635 5. (~~S//REL USA, AUS, GBR~~) USSTRATCOM. Facilitate (b)(1) Sec 1.4(a)

636 (b)(1) Sec 1.4(a)  
637

638 6. (U) JFCC GSI. (b)(1) Sec 1.7(e) IO capabilities as  
639 needed.  
640

641 c. (U) (b)(1) Sec 1.7(e) Activities in this (b)(1) Sec 1.7(e)

642 (b)(1) Sec 1.7(e)  
643  
644  
645

646 action in cyberspace.

647 d. (U) Coordinating Instructions

649 (1). (U) IO will be conducted through centralized planning and  
650 decentralized execution. JFCC GSI J39 will establish IO objectives and  
651 associated tasks. JFCC GSI J39 will coordinate IO plans and objectives with  
652 supporting commands, components, and support agencies.  
653

654 (2) (U) Supporting elements will give daily IO Situational Reports through  
655 the USSTRATCOM GOC providing the status of execution of supporting tasks  
656 in support of IO objectives.  
657

658 4. (U) Administration and Logistics. Refer to Base Plan.

660 a. (U) Forces utilized in this CONPLAN include deployable or fixed assets  
661 operating in CONUS or from sites located throughout the world and are  
662 controlled as separate forces. (b)(1) Sec 1.7(e)

663 (b)(1) Sec 1.7(e)  
664  
665

666 AOR. During a contingency, USSTRATCOM Service components will ensure all  
667 mission-critical cyberspace forces (fixed and mobile), are fully supported and  
668 capable of performing their mission.

669 5. (U) Command and Control

670 a. (U) Refer to Annex K (Command Control, Communications and Computer  
671 Systems), (b)(1) Sec 1.7(e)

672 b. (~~S//REL USA, AUS, GBR~~) Special IO Communication and Reporting  
673 Requirements. (b)(1) Sec 1.4(a)

674  
675  
676

587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630

6. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

7. (U) (b)(1) Sec 1.7(e)

8. (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

9. (U) (b)(1) Sec 1.7(e)

10. (U) (b)(1) Sec 1.7(e)

11. (U) (b)(1) Sec 1.7(e)

12. (U) (b)(1) Sec 1.7(e)

13. (U) Support activities establishing (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

14. (S//REL USA, AUS, GBR) Objective Balancing. When

(b)(1) Sec 1.4(a)

b. (U) (b)(1) Sec 1.7(e) Tasks

1. (U) Supporting CDRs. Employ IO options in support of USSTRATCOM (b)(1) Sec 1.7(e) objectives as directed. Maintain sufficient strategic reserve. (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

2. (S//REL USA, AUS, GBR) JTF GNO. Coordinate with supporting commanders, Service and functional components (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

3. (S//REL USA, AUS, GBR) JIOWC. Facilitate interagency coordination and integration (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

considered and made available to decision makers.

541 (b)(1) Sec 1.4(a)  
542

543  
544 5. (~~S//REL USA, AUS, GBR~~) JFCC GSI. Through the use of  
545 collaborative tools, (b)(1) Sec 1.4(a)

546 (b)(1) Sec 1.4(a)  
547  
548  
549

550  
551 c. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Activities in this

552 (b)(1) Sec 1.4(a)  
553  
554

555 cyberspace.

556  
557 (5) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The intent of this

558 (b)(1) Sec 1.4(a)  
559

560 (b)(1) Sec 1.4(a) operations if necessary. IO efforts (b)(1) Sec 1.4(a)

561 (b)(1) Sec 1.4(a)  
562  
563  
564  
565  
566

567  
568 a. (U) (b)(1) Sec 1.7(e) Strategic IO objectives. The following objectives

569 (b)(1) Sec 1.7(e)

570  
571 1. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

572 (b)(1) Sec 1.4(a)

573  
574 2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

575 (b)(1) Sec 1.4(a)

576  
577 3. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

578 (b)(1) Sec 1.4(a)  
579

580  
581 4. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

582 (b)(1) Sec 1.4(a)  
583

584  
585 5. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

586 (b)(1) Sec 1.4(a)

SECRET

495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540

(4). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

The intent of this

(b)(1) Sec 1.4(a)

a. (U) (b)(1) Sec 1.7(e) Strategic IO objectives

1. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

to other operations through cyberspace will be covered in (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2. (S//REL USA, AUS, GBR) Objective Balancing. When executing

(b)(1) Sec 1.4(a)

b. (U) (b)(1) Sec 1.7(e) Tasks

1. (U) Supporting CDRs. (b)(1) Sec 1.7(e)

USSTRATCOM cyberspace objectives as directed. (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

2. (S//REL USA, AUS, GBR) JTF-GNO. IAW published IA/CND

Plans coordinate with supporting commanders, Service and functional components to (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) essential elements of friendly information.

3. (S//REL USA, AUS, GBR) JFCC GSI/JFCC NW. Coordinate

(b)(1) Sec 1.4(a)

4. (S//REL USA, AUS, GBR) JIOWC. Facilitate interagency coordination and integration (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

SECRET

449 (b)(1) Sec 1.4(a)

450 actors.

451

452 2. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

453 (b)(1) Sec 1.4(a) OPLAN.

454

455 3. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

456 (b)(1) Sec 1.4(a) adversaries.

457

458 4. (U) Utilize IO to maximize effectiveness of force deployment,

459 (b)(1) Sec 1.7(e)

460

461 b. (U) (b)(1) Sec 1.7(e) Tasks

462

463 1. (U) Supporting CDRs. Employ IO options in support of  
464 USSTRATCOM cyberspace objectives as directed. (b)(1) Sec 1.7(e)

465 (b)(1) Sec 1.7(e)

466

467 2. (S//REL USA, AUS, GBR) JTF-GNO. IAW published IA/CND  
468 Plans coordinate with supporting commanders, Service and functional  
469 components to (b)(1) Sec 1.4(a)

470 (b)(1) Sec 1.4(a) essential elements of friendly information.

471

472 3. (S//REL USA, AUS, GBR) JFCC GSI/JFCC NW. Coordinate

473 (b)(1) Sec 1.4(a)

474

475 4. (S//REL USA, AUS, GBR) JIOWC. Facilitate interagency  
476 coordination and integration (b)(1) Sec 1.4(a)

477 (b)(1) Sec 1.4(a)

478

479 (U) 5. (S//REL USA, AUS, GBR) JFCC GSI. Collaborate with the  
480 effected GCC(s) and applicable agencies.

481

482 6. (S//REL USA, AUS, GBR) Objective Balancing. When executing

483 (b)(1) Sec 1.4(a)

484

485 c. (U) (b)(1) Sec 1.7(e) Activities in this (b)(1) Sec 1.7(e)

486 (b)(1) Sec 1.7(e) cyberspace mission(s).

487

SECRET

SECRET

404 | 1. (U) JTF GNO. Coordinate with supporting commanders, Service  
405 and functional components to develop robust IA to protect our critical  
406 information systems.

407  
408 2. (~~S//REL USA, AUS, GBR~~) JFCC GSI/JFCC NW. Identify,  
409 prioritize, and obtain (b)(1) Sec 1.4(a)  
410 (b)(1) Sec 1.4(a)  
411  
412 reflected in validated national collections requirements.

413  
414 3. (U) JFCC GSI/JIOWC. Facilitate interagency coordination and  
415 integration of appropriate (b)(1) Sec 1.7(e)  
416 (b)(1) Sec 1.7(e)  
417  
418 Through the use of collaborative tools, integrate planning actions (b)(1) Sec 1.7(e)  
419 (b)(1) Sec 1.7(e)  
420

421 4. (U) USSTRATCOM. Support US declaratory policy by preparing  
422 | CDRUSSTRATCOMs positions. Adjust force posture. Adjust themes and  
423 messages.

424  
425 (c). (U) (b)(1) Sec 1.7(e) Activities (b)(1) Sec 1.7(e)  
426 (b)(1) Sec 1.7(e)  
427  
428 (b)(1) Sec 1.7(e) in support of cyberspace mission(s).  
429

430 (3) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The intent of  
431 (b)(1) Sec 1.4(a)  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443

444 a. (U) (b)(1) Sec 1.7(e) Strategic IO objectives. Continue ongoing objectives  
445 (b)(1) Sec 1.7(e) following strategic objectives:

446  
447 1. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
448 (b)(1) Sec 1.4(a)

SECRET

SECRET

359 (c) (U) (b)(1) Sec 1.7(e) End State. Activities in this (b)(1) Sec 1.7(e)  
360 (b)(1) Sec 1.7(e) CDRUSSTRATCOM to present available IO COAs in support of  
361 cyberspace mission(s) (b)(1) Sec 1.7(e)  
362

363 (2) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
364 (b)(1) Sec 1.4(a)  
365  
366  
367  
368

369 force posture or execution of the identified options. IO actions conducted  
370 (b)(1) Sec 1.4(a)  
371  
372  
373 (b)(1) Sec 1.4(a) actions lead to achievement of US strategic objectives.  
374

375 (a). (U) (b)(1) Sec 1.7(e) Strategic IO Objectives. (b)(1) Sec 1.7(e) strategic  
376 objectives. Strategic Communication (SC) themes and messages will be  
377 situation dependant (b)(1) Sec 1.7(e)  
378 (b)(1) Sec 1.7(e)  
379  
380 consequences to the current adversarial government once their forces are  
381 neutralized.  
382

383 1. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
384 (b)(1) Sec 1.4(a)  
385  
386

387 2. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
388 (b)(1) Sec 1.4(a)  
389  
390

391 3. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
392 (b)(1) Sec 1.4(a)  
393

394 4. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
395 (b)(1) Sec 1.4(a)  
396 integrated to best achieve the commander's objectives.  
397

398 5. (S//REL USA, AUS, GBR) Objective Balancing. When executing  
399 (b)(1) Sec 1.4(a)  
400  
401

402 (b). (U) (b)(1) Sec 1.7(e) Tasks  
403



SECRET

315 (b)(1) Sec 1.4(a) Develop and  
316 manage IO COAs derived from the (b)(1) Sec 1.4(a)

317  
318 3. (S//REL USA, AUS, GBR) JFCC GSI/JFCC NW. (b)(1) Sec 1.4(a)

319 (b)(1) Sec 1.4(a)  
320  
321 (b)(1) Sec 1.4(a) necessary to accomplish detailed planning of IO options.  
322

323 4. (S//REL USA, AUS, GBR) JFCC GSI/JFCC NW. (b)(1) Sec 1.4(a)

324 (b)(1) Sec 1.4(a)  
325 Develop baseline force structure.

326  
327 5. (U) JTF-GNO. (b)(1) Sec 1.7(e)

328 (b)(1) Sec 1.7(e) USSTRATCOM information systems. Coordinate with supporting  
329 commanders, Service and functional components to develop robust IA and  
330 OPSEC plans to protect our critical information systems and essential elements  
331 of friendly information.  
332

333 6. (S//REL USA, AUS, GBR) JFCC GSI/JTF GNO. (b)(1) Sec 1.4(a)

334 (b)(1) Sec 1.4(a)

335  
336 7. (S//REL USA, AUS, GBR) JFCC GSI/Supporting CDRs. Develop

337 IO options (b)(1) Sec 1.4(a)  
338 (b)(1) Sec 1.4(a)  
339  
340  
341

342 8. (U) JIOWC. Facilitate interagency coordination and integration  
343 of appropriate IO themes, and responses to support objectives (b)(1) Sec 1.7(e)

344 Provide Combatant Commanders with IO support teams, integrate and  
345 coordinate (b)(1) Sec 1.7(e)

346 (b)(1) Sec 1.7(e)

347  
348 9. (U) USSTRATCOM, Services and Agencies

349  
350 a. (U) Identify and assist in development of IO capabilities  
351 necessary to meet validated requirements.  
352

353 b. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

354 (b)(1) Sec 1.4(a) of these issues.

355  
356 c. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

357 maintain situational awareness.  
358

270 b. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
271 (b)(1) Sec 1.4(a)  
272

273  
274 c. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
275 (b)(1) Sec 1.4(a)  
276  
277  
278

279  
280 9. (S//REL USA, AUS, GBR) Incorporate IO capabilities, as they  
281 become available (b)(1) Sec 1.4(a)  
282 (b)(1) Sec 1.4(a)  
283

284  
285 a. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) Develop and  
286 implement IO options which when (b)(1) Sec 1.4(a)  
287 (b)(1) Sec 1.4(a)  
288

289  
290 b. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
291 (b)(1) Sec 1.4(a)  
292  
293

294  
295 10. (S//REL USA, AUS, GBR) Objective Balancing. When  
296 executing (b)(1) Sec 1.4(a)  
297 (b)(1) Sec 1.4(a)  
298

299 (b). (U) (b)(1) Sec 1.7(e) Tasks

300  
301 1. (U) USSTRATCOM. (b)(1) Sec 1.7(e) USSTRATCOM  
302 staff and components, supporting commands and agencies are adequately  
303 trained in the IO disciplines needed to meet (b)(1) Sec 1.7(e)

304 (b)(1) Sec 1.7(e)  
305  
306  
307

308 (b)(1) Sec 1.7(e) Assess and identify IO capabilities against potential  
309 adversaries (b)(1) Sec 1.7(e) Support US declaratory policy by  
310 preparing CDRUSSTRATCOM positions. Establish IO requirements for  
311 CDRUSSTRATCOM-directed objectives.

312  
313 2. (S//REL USA, AUS, GBR) JFCC GSI. (b)(1) Sec 1.4(a)  
314 (b)(1) Sec 1.4(a)

226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) Key to success is working with supporting and component commands, Combatant Commanders and outside agencies on the integration and synchronization of the following strategic objectives:

(a). (U) (b)(1) Sec 1.7(e) IO Strategic Objectives

1. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) US is capable of (b)(1) Sec 1.4(a) networks.

2. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

3. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) adversaries.

4. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) adversaries.

5. (S//REL USA, AUS, GBR) Ensure friendly forces have (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

6. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) infrastructures.

7. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

8. (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

a. (S//REL USA, AUS, GBR) C4I Systems. (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a)

180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225

(a). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(b). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(2). (U) (b)(1) Sec 1.7(e)  
Example actions may include:

(a). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(b). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(3) (U) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) Example actions may include:

(a). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

(b). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

c. (U) (b)(1) Sec 1.7(e)

(1). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) The strategy of this  
(b)(1) Sec 1.4(a)

SECRET

134 (b)(1) Sec 1.7(e)

135 effects. It is important to note that IO plans that incorporate (b)(1) Sec 1.7(e)

136 (b)(1) Sec 1.7(e)  
137  
138

139 (b). (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

140 (b)(1) Sec 1.4(a)  
141

142 on the supporting information infrastructure. The DOD's (b)(1) Sec 1.4(a)

143 (b)(1) Sec 1.4(a)  
144  
145  
146  
147

148 Refer to Plan Summary, Base Plan and Annex C for more detailed descriptions  
149 of defense types.

151 (c). (~~S//REL USA, AUS, GBR~~) End State. Refer to the Base Plan and  
152 Annex C (Operations). (b)(1) Sec 1.4(a)

153 (b)(1) Sec 1.4(a)  
154  
155  
156  
157

158 (b)(1) Sec 1.4(a) and appropriate legal, informational, military, diplomatic or  
159 economic measures are taken (b)(1) Sec 1.4(a)

160 (b)(1) Sec 1.4(a)  
161  
162  
163

164 (b)(1) Sec 1.4(a) US resumes

165 normal cyber operations. (b)(1) Sec 1.4(a)

166 (b)(1) Sec 1.4(a)  
167 DOD is  
168 postured to support homeland security, critical infrastructure protection, and  
169 civil support. US, allies, and coalition partners have freedom of action to  
170 operate in cyberspace.

172 (d). (U) Cyber Engagement Criteria. Refer to the Base Plan.

174 b. (U) Strategic Objectives/IO Tasks. General IO tasks will be covered in  
175 Tabs A through G of Appendix 3 (Information Operations). All types of cyber  
176 defense will be utilized (b)(1) Sec 1.7(e)

178 (1). (U) (b)(1) Sec 1.7(e)

179 (b)(1) Sec 1.7(e) Example actions may include:

88 IO (b)(1) Sec 1.4(a) Additionally, USSTRATCOM

89 (b)(1) Sec 1.4(a)  
90  
91  
92

93 (2) (S//REL USA, AUS, GBR) The commander's IO efforts will (b)(1) Sec 1.4(a)

94 (b)(1) Sec 1.4(a) by employing assigned IO  
95 assets to protect USSTRATCOM information from (b)(1) Sec 1.4(a)

96 (b)(1) Sec 1.4(a) while ensuring readiness, reliability,  
97 and continuity of the DOD GIG and the critical information infrastructure. IO

98 (b)(1) Sec 1.4(a)  
99  
100  
101  
102

103 (a). (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

104 (b)(1) Sec 1.4(a)

105  
106 1. (U) COAs. (b)(1) Sec 1.7(e)

107 (b)(1) Sec 1.7(e)  
108 The primary method of supporting the mission is through the development of  
109 integrated IO courses of action (b)(1) Sec 1.7(e)

110 (b)(1) Sec 1.7(e)  
111  
112

113 (b)(1) Sec 1.7(e) courses of action underscore  
114 the importance of contingency planning and early response to a crisis. Given  
115 clearly stated objectives and effectively integrated IO capabilities, this has the  
116 potential to change the course of threatening events. Finally, when deterrence  
117 fails, IO (b)(1) Sec 1.7(e) COA. Refer to

118 Figure C-3-1.

119  
120 2. (U) (b)(1) Sec 1.7(e)

121 (b)(1) Sec 1.7(e) Specific

122 implementation supporting (b)(1) Sec 1.7(e)

123 (b)(1) Sec 1.7(e) to

124 Appendix 3 (Information Operations) to Annex C (Operations). (b)(1) Sec 1.7(e)

125 (b)(1) Sec 1.7(e)  
126  
127  
128  
129  
130  
131  
132  
133

SECRET

42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) This appendix provides guidance for the planning, integration and implementation of current IO capabilities and development of future IO capabilities to support the planning, deployment and employment of US forces for dominance in cyberspace. (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

a. (U) Adversary. Refer to Annex B (Intelligence) (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

b. (U) Friendly. Refer to the Base Plan.

(1) (U) The US and our allies are increasingly reliant on automated communications and information-based decision-making systems. These systems are vital to US warfighting capabilities. The US requires an integrated and synchronized approach to maintaining information superiority.

(2) (U) Essential Elements of Friendly Information. Refer to the Base Plan.

c. (U) Assumptions. Refer to the Base Plan.

2. (U) Mission. Refer to the Base Plan.

3. (U) (b)(1) Sec 1.7(e)

a. (~~S//REL USA, AUS, GBR~~) Concept of Operations. This appendix provides USSTRATCOM with (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) US vital interests and contribute to conflict termination on terms favorable to the US.

(1) [~~S//REL~~] This appendix provides a variety of preplanned courses of action (COA) that support CDRUSSTRATCOM objectives outlined in the Base Plan. (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) US and coalition forces. USSTRATCOM will coordinate, integrate, and synchronize DOD IO in support of assigned cyberspace missions, identify IO requirements and capabilities for cyber operations and, when directed, plan and or execute

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NEBRASKA 68113-6500  
28 February 2008

APPENDIX 3 TO ANNEX C TO CDRUSSTRATCOM CONPLAN 8039 (U)

(U) OPR: JFCC GSI J39

INFORMATION OPERATIONS (U)

(U) References: Refer to Base Plan.

a. (U) CJCSI 3210.01B, Joint Information Operations Policy, 5 January 07 (S)

b. (U) DODD-3600.01 Information Operations, 14 Aug 06 (U)

c. (U) Joint Pub 3-13.1 Joint Doctrine for Electronic Warfare, 25 Jan 2007 (U)

d. (U) Joint Pub 3-13, Information Operations, 13 Feb 2006 (U)

e. (U) (b)(1) Sec 1.7(e) 13 Jul 06 (U)

f. (U) (b)(1) Sec 1.7(e) 01 Aug 2007 (S)

g. (U) CJCSI 3210.03B, Joint Electronic Warfare Policy, 31 Jul 02 (S)

h. (U) JP 3-13.3 Joint Doctrine for Operations Security, 29 Jun 06 (U)

i. (U) (b)(1) Sec 1.7(e) 5 Sep 2003 (U)

k. (U) JP 3-09, Doctrine for Joint Fire Support, 13 Nov 2006 (U)

k. (U) JP 3-61, Joint Doctrine for Public Affairs, 9 May 2005 (U)

l. (U) (b)(1) Sec 1.7(e) Jan 2006 (S//NF)

1. (~~S//REL USA, AUS, GBR~~) Situation. This appendix describes IO activities supporting USSTRATCOM's CONPLAN 8039. IO integrates the core capabilities of OPSEC, (b)(1) Sec 1.4(a) and CNO to achieve CDRUSSTRATCOM effects and objectives (b)(1) Sec 1.4(a) to fulfill this plans objectives.

~~Classified by: Multiple Sources  
Reason: 1.4(a), (e), and (g)  
Declassify on: 26 February 2032~~

When employed successfully, IO (b)(1) Sec 1.4(a)



**SECRET**

265 (b)(1) Sec 1.4(a)  
266

267 (8) (U) Tasks. Refer to Base Plan for additional tasks and (b)(1) Sec 1.7(e)

268 (b)(1) Sec 1.7(e)

269 (b)(1) Sec 1.7(e) For CONPLAN 8039 taskings, significant interagency support  
270 may be required. Access to the interagency will be through the Joint Staff  
271 or appropriate liaison elements. Refer to Annex V (Interagency  
272 Coordination) for further discussion. This CONPLAN will not explicitly  
273 task the interagency partners.

274 (9) (U) Coordinating Instructions. Refer to Base Plan.

275

276 4. (U) Administration and Logistics. Refer to the Base Plan.

277

278 5. (U) Command and Control. Refer to the Base Plan and Annex J  
279 (Command Relationships).

280

281

282 OFFICIAL

283

284

285 s/

286 Mark H. Owen

287 Brigadier General, USAF

288 Director, Plans and Policy

289

290

291

292 KEVIN CHILTON

293 General, USAF

294 Commander

295

296

297

298 Appendixes:

299 3 -- Information Operations

300 8 -- Rules of Engagement

301 9 -- Intelligence, Surveillance and Reconnaissance

302 16 -- Critical Infrastructure Protection

303 17 -- Network Operations

304 18 -- Time Sensitive Planning

305 19 -- Effect Assessment Guidance

306 20 -- (b)(1) Sec 1.7(e)

**SECRET**

**SECRET**

230 2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
231 operations favor: (b)(1) Sec 1.4(a)  
232 (b)(1) Sec 1.4(a) Refer to (b)(1) Sec 1.4(a) should consider the impact that a  
233 (b)(1) Sec 1.4(a)

234 (d). (U) (b)(1) Sec 1.7(e)

235 1. (~~S//REL USA, AUS, GBR~~) Commander's Intent. (b)(1) Sec 1.4(a)  
236 (b)(1) Sec 1.4(a)  
237  
238  
239  
240  
241

242 2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
243 operations favor: (b)(1) Sec 1.4(a)  
244 (b)(1) Sec 1.4(a)  
245

246 (e). (U) (b)(1) Sec 1.7(e)

247 1. (~~S//REL USA, AUS, GBR~~) Commander's Intent. (b)(1) Sec 1.4(a)  
248 (b)(1) Sec 1.4(a)  
249  
250

251 2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
252 operations favor: (b)(1) Sec 1.4(a) The  
253 planner should consider (b)(1) Sec 1.4(a)  
254 (b)(1) Sec 1.4(a)  
255  
256

257 (f). (U) (b)(1) Sec 1.7(e)

258 1. (~~S//REL USA, AUS, GBR~~) Commander's Intent. Provide  
259 (b)(1) Sec 1.4(a)  
260

261 2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
262 operations favor (b)(1) Sec 1.4(a)  
263 (b)(1) Sec 1.4(a)  
264

**SECRET**

**SECRET**

195 (U)(e) (~~S//REL USA, AUS, GBR~~) Intelligence, Surveillance, and  
196 Reconnaissance (ISR) Operations. Refer to Appendix 9 (Intelligence,  
197 Surveillance and Reconnaissance) to Annex C (Operations).

198 (f) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

199 (b)(1) Sec 1.4(a)

200 (7) (U) Cyberspace (b)(1) Sec 1.7(e)

201 (a). (U) (b)(1) Sec 1.7(e)

202 1. (~~S//REL USA, AUS, GBR~~) Commander's Intent. Support  
203 US government efforts to (b)(1) Sec 1.4(a)

204 (b)(1) Sec 1.4(a)

207 2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

208 (b)(1) Sec 1.4(a)

211 US national interests if attributed.

212 (b). (U) (b)(1) Sec 1.7(e)

213 1. (~~S//REL USA, AUS, GBR~~) Commander's Intent. (b)(1) Sec 1.4(a)

214 (b)(1) Sec 1.4(a)

218 2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

219 (b)(1) Sec 1.4(a)

221 (b)(1) Sec 1.4(a) US national interests if  
222 attributed.

223 (c). (U) (b)(1) Sec 1.7(e)

224 1. (~~S//REL USA, AUS, GBR~~) Commander's Intent. (b)(1) Sec 1.4(a)

225 (b)(1) Sec 1.4(a)

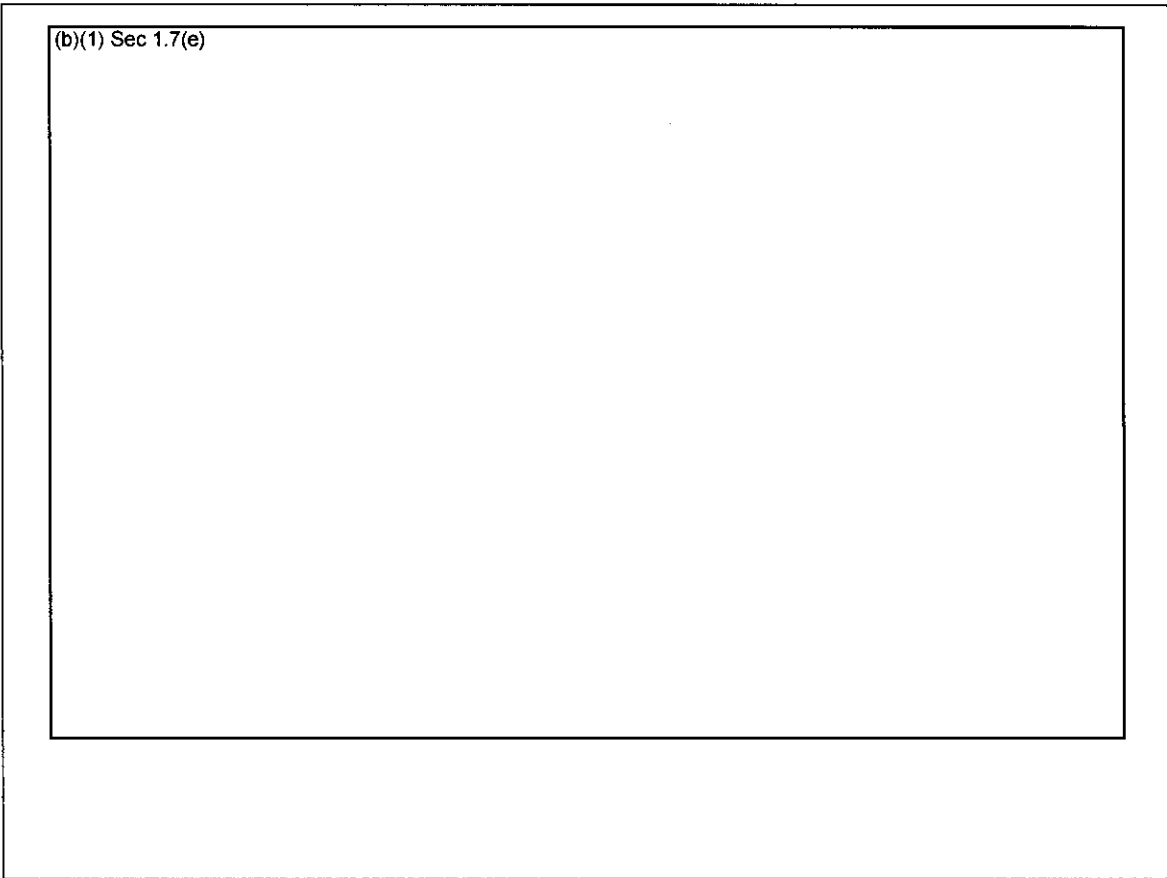


Figure 6: (U) Sample (b)(1) Sec 1.7(e) Activities

177

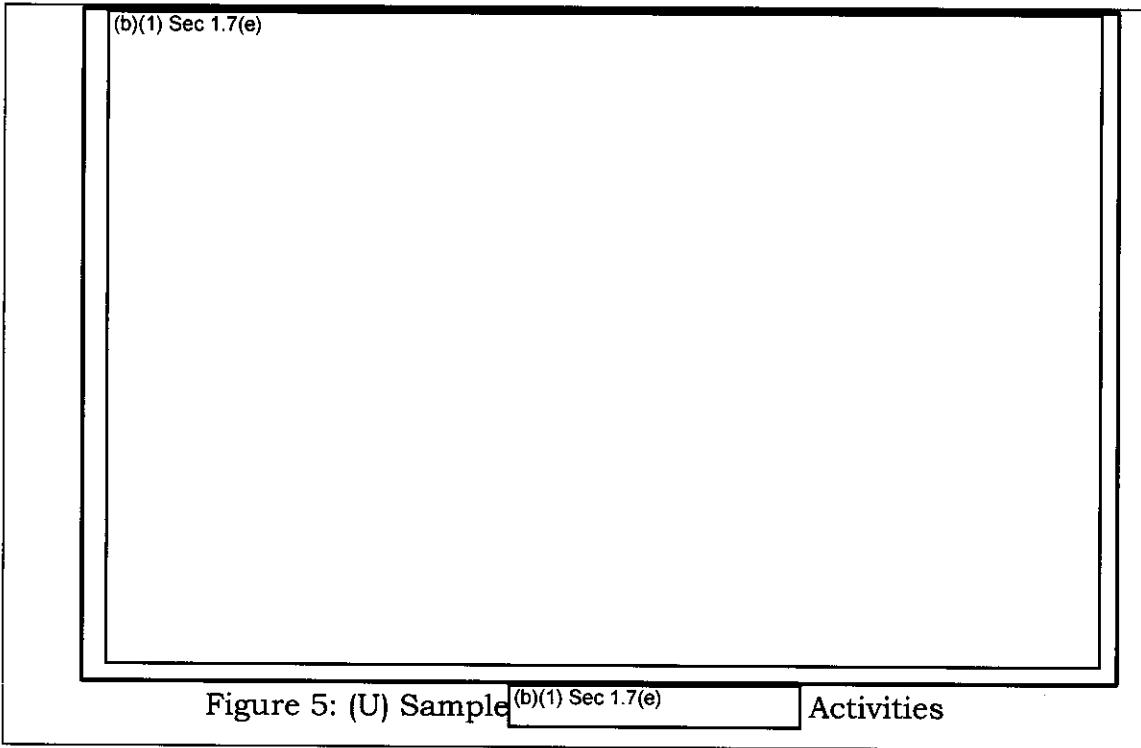
178 (6). (U) Supporting capabilities. In addition to USSTRATCOM's  
 179 cyberspace capabilities, supporting capabilities will be synchronized to  
 180 achieve (b)(1) Sec 1.7(e) within  
 181 (b)(1) Sec 1.7(e) While each plan (b)(1) Sec 1.7(e)  
 182 (b)(1) Sec 1.7(e) there  
 183 are capabilities that should be considered in any plan.

184 (a) (U) Strategic Communication. Refer to Annex Y (Strategic  
 185 Communication)

186 (b) (U) (b)(1) Sec 1.7(e) Refer to Appendix 3  
 187 (b)(1) Sec 1.7(e) to Annex A (Task Organization) for general  
 188 (b)(1) Sec 1.7(e) guidance (b)(1) Sec 1.7(e)  
 189 (b)(1) Sec 1.7(e)

190 (c) (U) Information Operations (IO). Refer to Appendix 3  
 191 (Information Operations) of Annex C (Operations) for detailed discussion of  
 192 the integration of each core IO capabilities in support of CONPLAN 8039.

193 (d) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) Refer to Annex  
 194 (b)(1) Sec 1.4(a)



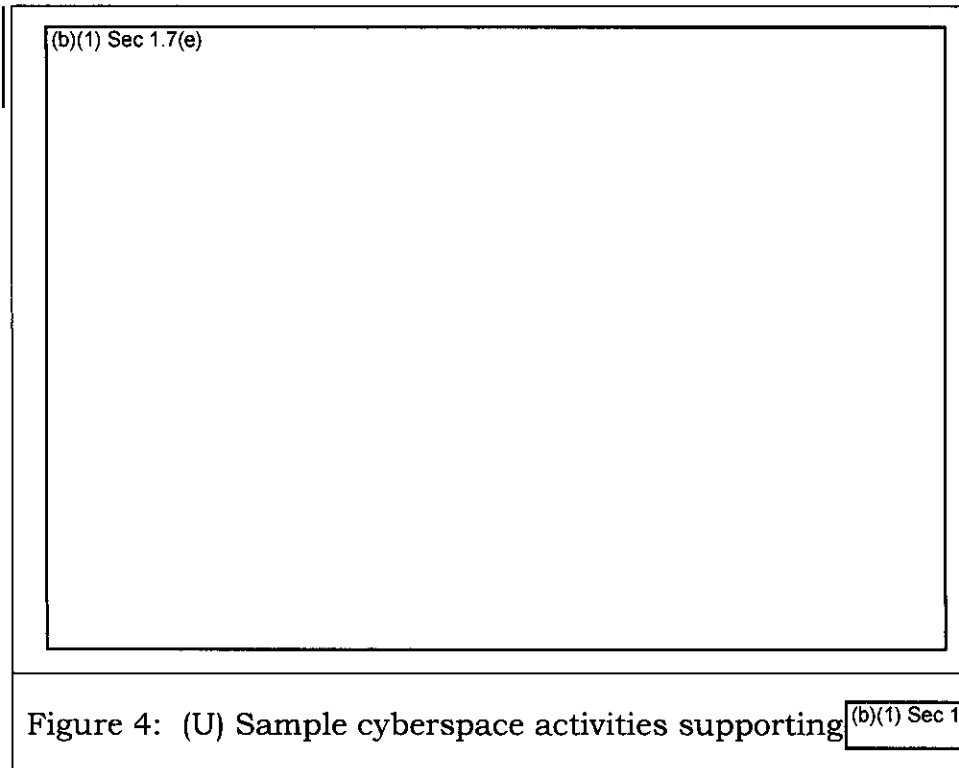
165

166

167 (d) (U) (b)(1) Sec 1.7(e) in support of operations in and  
168 through cyberspace includes (b)(1) Sec 1.7(e)  
169 (b)(1) Sec 1.7(e)  
170  
171 (b)(1) Sec 1.7(e) including other aspects of IO. See Figure 6  
172 below for sample (b)(1) Sec 1.7(e) to  
173 Appendix 3 (Information Operations) to Annex C (Operations) for  
174 additional discussion.

175

176



153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164

(c) (U) (b)(1) Sec 1.7(e) can come from any  
(b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e) to Appendix 3 (Information Operations) to Annex C  
(Operations) for additional discussion.

144 3 as a construct for a notional adversary. This process should be followed

145 (b)(1) Sec 1.7(e) designated in (b)(1) Sec 1.7(e)

146 (b)(1) Sec 1.7(e)

147

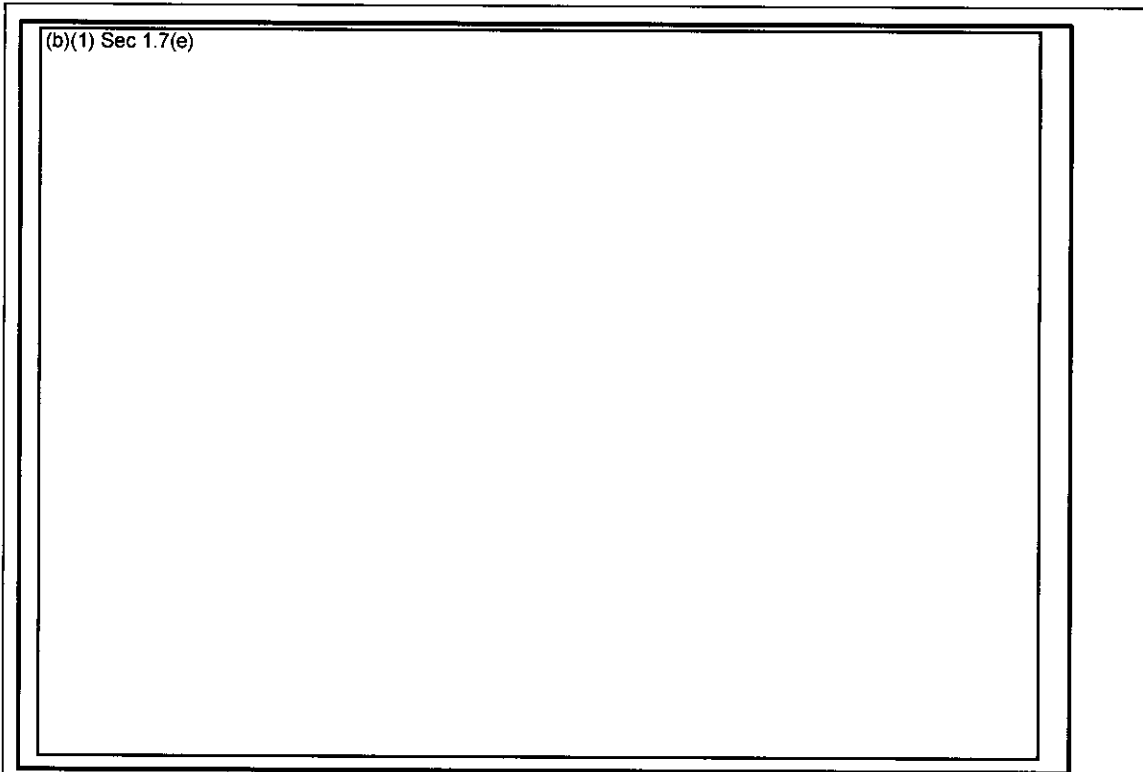


Figure 3: (U) Sample cyberspace activities supporting (b)(1) Sec 1.7(e)

148 (b). U (b)(1) Sec 1.7(e)

149 (b)(1) Sec 1.7(e)

150

151 other command plans as applicable. Consider Figure 4 as a construct  
152 where other commanders (or other USSTRATCOM plans) are supported.

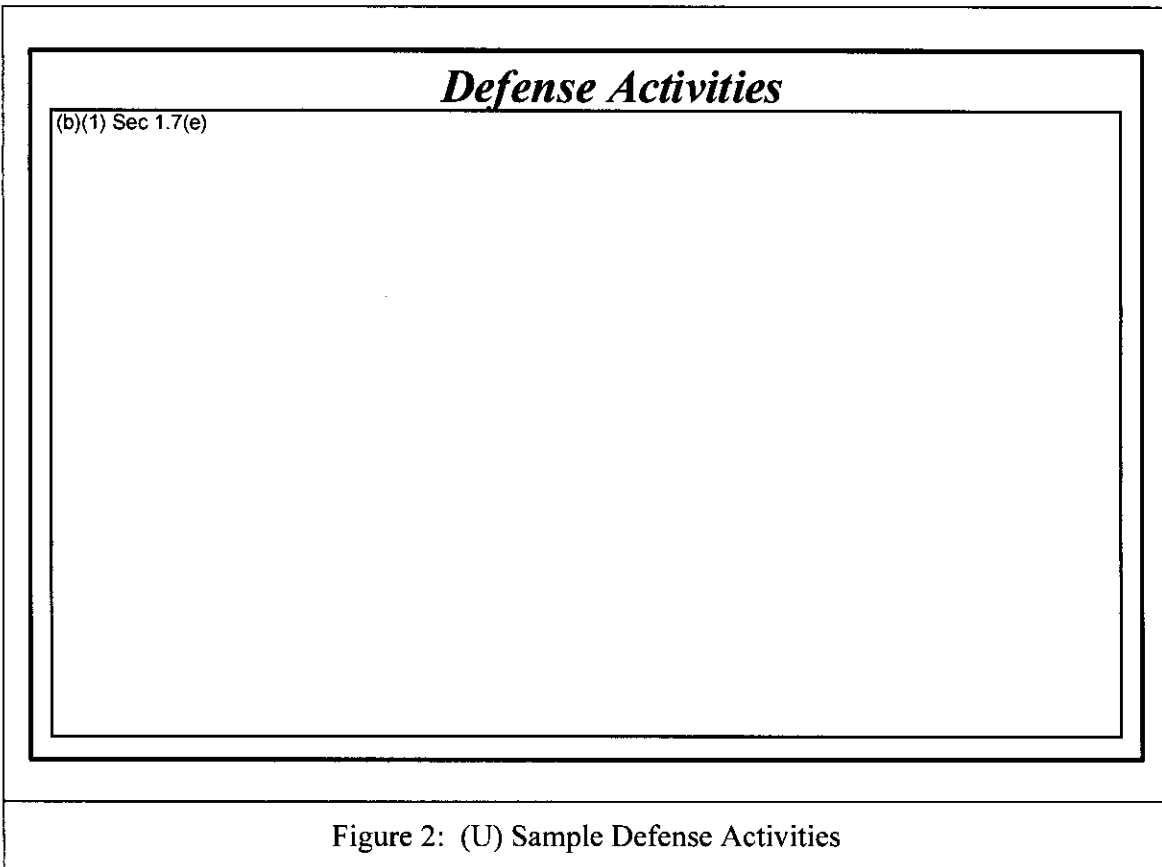


Figure 2: (U) Sample Defense Activities

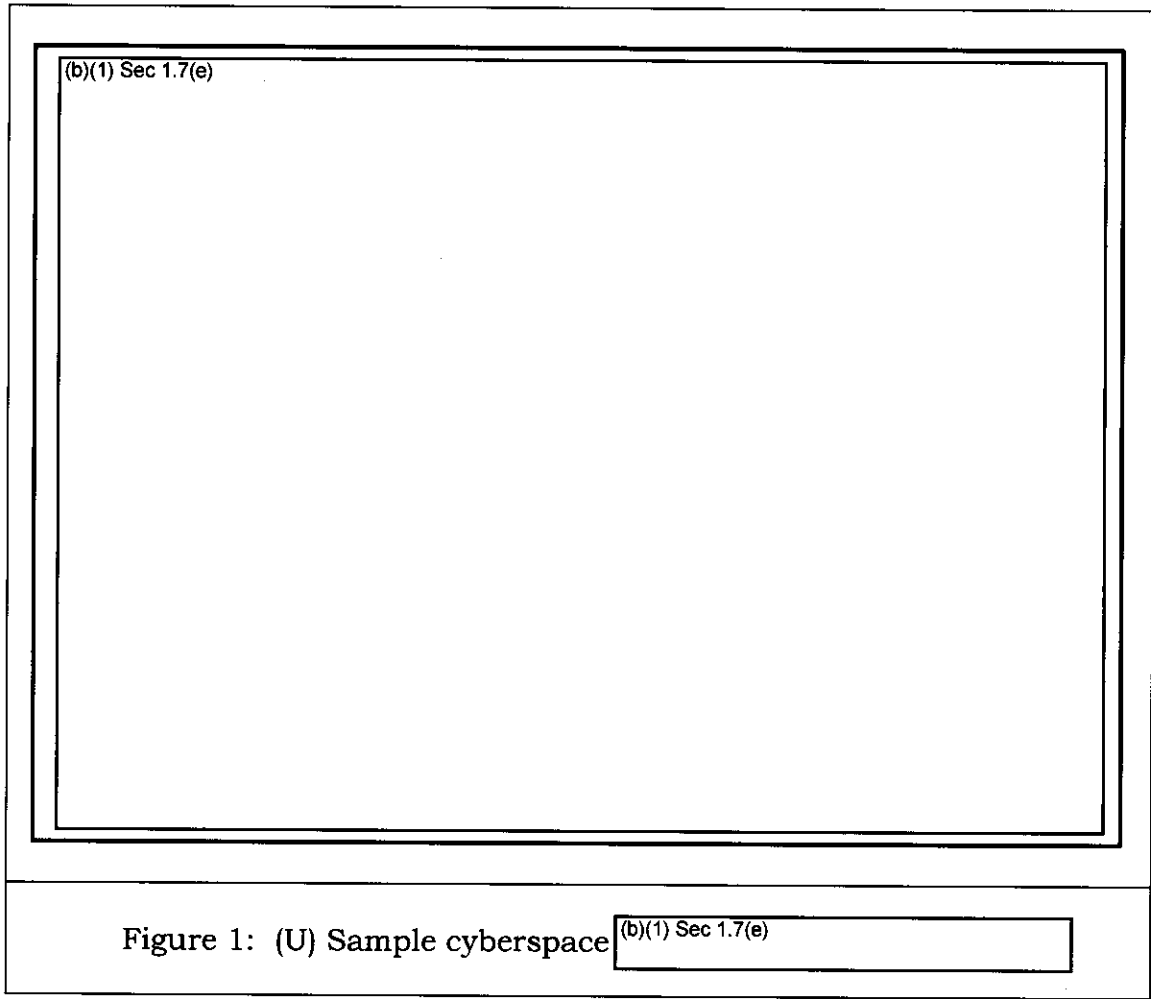
123 (5) Offensive Operations in and through cyberspace. USSTRATCOM  
 124 will provide a range of offensive capabilities in the cyberspace domain to  
 125 achieve (b)(1) Sec 1.7(e)

126 (b)(1) Sec 1.7(e)  
 127  
 128  
 129  
 130  
 131

132 can be supported by or in support of (b)(1) Sec 1.7(e)  
 133 environments. Specific activities should be planned (b)(1) Sec 1.7(e)  
 134 operations. See (b)(1) Sec 1.7(e) for  
 135 (b)(1) Sec 1.7(e) see  
 136 (b)(1) Sec 1.7(e) to Appendix 3 (Information Operations) to  
 137 Annex C (Operations). For purposes of this CONPLAN, in accordance with  
 138 (b)(1) Sec 1.7(e) are described as below in  
 139 (b)(1) Sec 1.7(e)

140 (a) (U) (b)(1) Sec 1.7(e)  
 141 (b)(1) Sec 1.7(e) will be integrated across each of their  
 142 military functions. (b)(1) Sec 1.7(e)  
 143 (b)(1) Sec 1.7(e) Consider Figure





SECRET

78 the effects that they could create across all sub-areas of cyberspace (A  
79 through E as outlined in Figure 1 of the Base Plan). USSTRATCOM will  
80 plan and conduct operations in cyberspace, to achieve CONPLAN 8039  
81 objectives. The desired effects list found in paragraph 3b(3)(c)2d assist  
82 Combatant Commands in establishing a framework to (b)(1) Sec 1.7(e) with  
83 specific tasks that cyber forces will execute. The (b)(1) Sec 1.7(e)

84 (b)(1) Sec 1.7(e)  
85  
86

87 (b)(1) Sec 1.7(e)

88 (3) (U) Offense Defense Mix. To achieve cyberspace superiority,  
89 forces require situational awareness, robust defense in depth of our  
90 cyberspace systems, the ability (b)(1) Sec 1.7(e)  
91 (b)(1) Sec 1.7(e) commander's  
92 intent. (b)(1) Sec 1.7(e)

93 (b)(1) Sec 1.7(e) These activities are not conducted (b)(1) Sec 1.7(e)  
94 (b)(1) Sec 1.7(e)  
95

96 improve their defenses. Offensive and defensive capabilities will be merged  
97 in CONPLAN 8039 to establish cyberspace superiority at times and places  
98 critical to the accomplishment (b)(1) Sec 1.7(e)

99 (4) (U) Defensive Operations in cyberspace. CONPLAN 8039  
100 describes cyberspace defense as those actions taken in cyberspace to  
101 protect, defend, monitor, analyze, detect and respond to unauthorized  
102 attacks against the DOD GIG, and as directed, other US cyberspace. For  
103 purposes of this CONPLAN, in accordance with (b)(1) Sec 1.4(a),  
104 guidance, defensive operations are described as below.

105 (a). (U//FOUO) (b)(1) Sec 1.7(e)

106 (b)(1) Sec 1.7(e)  
107  
108

109 cyberspace. (b)(1) Sec 1.7(e) planners will  
110 consider (b)(1) Sec 1.7(e)  
111 (b)(1) Sec 1.7(e)

112 (b)(1) Sec 1.7(e)  
113 Planners will also consider friendly  
114 (b)(1) Sec 1.7(e)

115 cyberspace. Consider Figure 1 as a construct to ensure (b)(1) Sec 1.7(e)

116 (b)(1) Sec 1.7(e) This process of developing operations  
117 in and through cyberspace (b)(1) Sec 1.7(e)  
118 military functions should be followed for a (b)(1) Sec 1.7(e)  
119 designated in (b)(1) Sec 1.7(e)

120 Figure 2 describes (b)(1) Sec 1.7(e)

SECRET

**SECRET**

38 obligations to which the US is a party, LOAC, customary international law,  
39 ROEs, and national policies.

40 2. (U) Mission. Refer to Base Plan.

41 3. (U) Execution

42 a. (~~S//REL USA, AUS, GBR~~) Conduct of Operations. Operations in  
43 and through cyberspace (b)(1) Sec 1.4(a)

44 (b)(1) Sec 1.4(a)

46 CDRUSSTRATCOM will provide strategic direction to CC/S/As for  
47 (b)(1) Sec 1.4(a) in and through cyberspace.

48 CDRUSSTRATCOM may establish a (b)(1) Sec 1.4(a) to

49 (b)(1) Sec 1.4(a)

50 (b)(1) Sec 1.4(a) USSTRATCOM's JFCC GSI, JFCC NW) and  
51 JTF GNO will coordinate all requests from CC/S/As, prioritize these  
52 requests and coordinate for support from the applicable CC/S/As as  
53 needed. US military operations in cyberspace will be conducted as  
54 necessary to (b)(1) Sec 1.4(a)

55 (b)(1) Sec 1.4(a)

60 when directed.

61 (1) (U) Commander's Intent. USSTRATCOM conducts operations in  
62 and through cyberspace by providing cyberspace effects under two  
63 scenarios:

64 (a) When CDRUSSTRATCOM is the supported commander for  
65 planning within the context of other STRATCOM plans (b)(1) Sec 1.7(e)

66 (b)(1) Sec 1.7(e)

67 In this case, cyberspace effects will  
68 also (b)(1) Sec 1.7(e) Additionally,

68 when supported, CDRUSSTRATCOM will provide cyberspace effects to

69 (b)(1) Sec 1.7(e)

70 (b) When USSTRATCOM is a supporting commander for another  
71 combatant commander, effects and activities in support of other plans will  
72 be derived via the applicable combatant commander plan. For timing and  
73 tempo of operations, USSTRATCOM-assigned forces will follow the phasing  
74 or planned construct resident in that plan.

75 (2) (U) Priority Effects. Refer to the Base Plan. (b)(1) Sec 1.7(e)

76 (b)(1) Sec 1.7(e)

77 Therefore all operations in and through cyberspace must be considered for

**SECRET**

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AFB NE 68113-6500  
28 February 2008

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37

ANNEX C TO USSTRATCOM CONPLAN 8039 (U)

(U) OPR: JFCC NW J5

OPERATIONS (U)

(U) References: Refer to Base Plan.

1. (U) Situation

a. (~~S//REL USA, AUS, GBR~~) General.

(1) (~~S//REL USA, AUS, GBR~~) CONPLAN 8039 describes the process for planning and (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) This annex discusses the concept of operations for (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) command relationships and (b)(1) Sec 1.4(a) military operations relative to

CDRUSSTRATCOM mission to conduct DOD operations in and through cyberspace. This annex discusses (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) Plans concerning (b)(1) Sec 1.4(a) (b)(1) Sec 1.4(a) of this

plan.

(2) (U) (b)(1) Sec 1.7(e) in cyberspace are currently centered on (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) However (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

b. (U) Area of Concern. See Base Plan.

c. (U) (b)(1) Sec 1.7(e) See Base Plan

d. (U) Adversary Capabilities. See Base Plan

e. (U) Friendly Force Capabilities. See Base Plan. .

(1) (U) Assumptions. See Base Plan.

(U) f. (~~C//REL~~) Legal Considerations. See Appendix 8 (Rules of Engagement). Legal review is required in the planning and execution of operations in and through cyberspace to ensure compliance with the US Constitution, applicable US statutes, international treaty/agreement

~~SECRET~~

(INTENTIONALLY BLANK)

~~SECRET~~

B-9-4

SECRET

72 (2) (U) The USSTRATCOM/J3 approves requests and (b)(1) Sec 1.7(e)  
73 (b)(1) Sec 1.7(e) as recommended by the USSTRATCOM/ J2.

74 (3) (U) The USSTRATCOM (b)(1) Sec 1.7(e)  
75 (b)(1) Sec 1.7(e)

76 (4) (U) Components will secure and maintain (b)(1) Sec 1.7(e)  
77 identified in paragraph 1.

78 c. (U) Coordinating Instructions. DIRLAUTH is authorized between all  
79 coordinating units and the Headquarters USSTRATCOM staff.

80 4. (U) Administration and (b)(1) Sec 1.7(e)  
81 administrative processing of (b)(1) Sec 1.7(e)

82 a. (U) (b)(1) Sec 1.7(e)  
83 (b)(1) Sec 1.7(e)  
84

85 b. (U) Administration. Administrative control (b)(1) Sec 1.7(e)  
86 (b)(1) Sec 1.7(e) and proper reporting are vital parts of the process. (b)(1) Sec 1.7(e)  
87 (b)(1) Sec 1.7(e) is initially published for National-level  
88 consumption and archived at the (b)(1) Sec 1.7(e) Contents of the initial report  
89 consist of lead examiner, date of report, (b)(1) Sec 1.7(e)  
90 (b)(1) Sec 1.7(e)  
91  
92

93 5. (U) Command and Control. (b)(1) Sec 1.7(e)  
94 (b)(1) Sec 1.7(e) would notify their higher headquarters to inform  
95 them of (b)(1) Sec 1.7(e) They would then immediately implement (b)(1) Sec 1.7(e) and  
96 administrative procedures.

97  
98 Kevin P. Chilton  
99 General, USAF  
100 COMMANDER

SECRET

30 2. (U) Mission. Refer to Basic Plan.

31 3. (U) Execution

32 a. (U) Concept of Operations. Summarize the general concept governing

33 (b)(1) Sec 1.7(e)

34 (b)(1) Sec 1.7(e) The following topics are covered specifically in  
35 Tabs to this Appendix.

36 (1) (~~S//REL USA, AUS, GBR~~) Upon execution of CONPLAN 8039,  
37 CDRUSSTRATCOM will (b)(1) Sec 1.4(a)

38 (b)(1) Sec 1.4(a)  
39  
40  
41

42 (b)(1) Sec 1.4(a) for USSTRATCOM. USSTRATCOM subordinate commanders  
43 will report the (b)(1) Sec 1.4(a) to USSTRATCOM/ J2 for  
44 (b)(1) Sec 1.4(a) USSTRATCOM/ J2 (b)(1) Sec 1.4(a)  
45 (b)(1) Sec 1.4(a) to satisfy CDRUSSTRATCOM intelligence  
46 requirements.

47 (2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) through

48 (b)(1) Sec 1.4(a)  
49  
50

51 (b)(1) Sec 1.4(a) through legal channels.

52 (3) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

53 (b)(1) Sec 1.4(a)  
54 (b)(1) Sec 1.4(a) are of great value to USSTRATCOM's IO mission and force  
55 protection operations. In addition, (b)(1) Sec 1.4(a)  
56 (b)(1) Sec 1.4(a) may provide significant  
57 information for USSTRATCOM and President and Secretary of Defense.  
58 (b)(1) Sec 1.4(a)  
59

60 b. (U) Tasks. (b)(1) Sec 1.7(e)

61 (b)(1) Sec 1.7(e)  
62  
63

64 (b)(1) Sec 1.7(e) List the assigned tasks to  
65 each element of the supported and supporting commands. At a minimum  
66 address tasks for J-2, J-3, (b)(1) Sec 1.7(e)  
67 (b)(1) Sec 1.7(e) and component commands.

68 (1) (U) The USSTRATCOM/J2 is responsible for leadership, oversight,  
69 and policy of (b)(1) Sec 1.7(e) The USSTRATCOM/J2 prioritizes (b)(1) Sec 1.7(e)  
70 requirements, operationally controls the (b)(1) Sec 1.7(e)  
71 intelligence.

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AFB NE 68113-6500  
26 February 2008

1 APPENDIX 9 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039-07 (U)

2 (U) OPR: HQ USSTRATCOM J2

3 (b)(1) Sec 1.7(e) USSC (U)

5 (U) References:

6 a. (U) (b)(1) Sec 1.7(e) " 18 Sep 86, (C).

7 b. (U) (b)(1) Sec 1.7(e) " 30  
8 Jun 97 (U).

9 c. (U) (b)(1) Sec 1.7(e)

10 (b)(1) Sec 1.7(e) " Aug 87 (U).

11 d. (U) Joint Pub 2-01, Intelligence Support to Joint Operations, 20 Nov 96,  
12 (U).

13 1. ~~(S//REL USA, AUS, GBR)~~ Situation. (b)(1) Sec 1.4(a)

14 (b)(1) Sec 1.4(a)

17 discovery. The information obtained assists in (b)(1) Sec 1.4(a)

18 (b)(1) Sec 1.4(a) They also provide key information for the (b)(1) Sec 1.4(a)

19 (b)(1) Sec 1.4(a) It is therefore vital (b)(1) Sec 1.4(a)

20 (b)(1) Sec 1.4(a)

22 a. (U) (b)(1) Sec 1.7(e) Refer to Annex B of the Base Plan (b)(1) Sec 1.7(e)

23 (b)(1) Sec 1.7(e)

24 b. ~~(S//REL USA, AUS, GBR)~~ Friendly. USSTRATCOM/ J2 will provide  
25 guidance and support (b)(1) Sec 1.4(a)

26 (b)(1) Sec 1.4(a)

28 c. (U) Assumptions. Some (b)(1) Sec 1.7(e)

29 (b)(1) Sec 1.7(e)

Classified by: Multiple Sources  
Reason: 1.4(a), (e), and (g)  
Declassify on: 26 February 2032



~~SECRET~~

188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211

(PAGE INTENTIONALLY LEFT BLANK)

~~SECRET~~

B-8-6

~~SECRET~~

176 (3) (U) USSTRATCOM Collection Managers can select alternate product  
177 delivery methods within (b)(1) Sec 1.7(e)

178

179 5. (U) Command and Control. Refer to Annex B (Intelligence)

180

181

182 Kevin P. Chilton

183 General, USAF

184 COMMANDER

185

186

187

~~SECRET~~

B-8-5

SECRET

(c) (U) Provide immediate information on and assessments (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(d) (U) Provide updates and status concerning changes that affect the

(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) to facilitate the most responsive tasking of assets in support of Commander, USSTRATCOM.

(e) (U) (b)(1) Sec 1.7(e) support of

USSTRATCOM collection requirements.

(3) (U) (b)(1) Sec 1.7(e) through the

(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) USSTRATCOM standing requirements validated by

(b)(1) Sec 1.7(e) Refer to reference b.

(4) (U) USSTRATCOM JFCC ISR. Ensure proper national-level coordination and approval of appropriate (b)(1) Sec 1.7(e) requirements in support of this CONPLAN.

(5) (U) USSTRATCOM (b)(1) Sec 1.7(e) Assist in monitoring the progress of (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) requirements and product reporting.

c. (U) Coordinating Instructions. Refer to references a through i.

4. (U) Administration and Logistics

a. (U) Logistics. Not applicable.

b. (U) Reporting

(1) (U) (b)(1) Sec 1.7(e) task appropriate processing and (b)(1) Sec 1.7(e) to satisfy validated USSTRATCOM requirements. This will be accomplished through (b)(1) Sec 1.7(e)

(2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

product format or posting location. Refer to references b and g.

SECRET

85 (1) (U) Collection Management. USSTRATCOM/J2 will provide (b)(1) Sec 1.7(e)  
86 (b)(1) Sec 1.7(e) support to HQs staff elements only. USSTRATCOM  
87 JFCCs, Centers, components, and subordinate commands will assume (b)(1) Sec 1.7(e)  
88 (b)(1) Sec 1.7(e) functions for their organizations while keeping HQ  
89 informed. JFCC ISR will closely collaborate with USSTRATCOM/J2 to  
90 maintain awareness of requirements and to ensure synchronization with DOD  
91 ISR. Ultimately, reporting agencies will be responsible to the Command and its  
92 subordinate JFCCs.

93  
94 (2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) The DOD  
95 architecture for (b)(1) Sec 1.4(a)  
96 distributed throughout the DOD. (b)(1) Sec 1.4(a)  
97 support USSTRATCOM missions are executed by other organizations, to  
98 include (b)(1) Sec 1.4(a)

99  
100 b. (U) Tasks

101  
102 (1) (U) USSTRATCOM Collection Managers

103  
104 (a) (U) USSTRATCOM/J23 Collection Managers submit (b)(1) Sec 1.7(e)  
105 requirements (b)(1) Sec 1.7(e)  
106 (b)(1) Sec 1.7(e) Refer to reference c.

107  
108 (b) (U) USSTRATCOM JFCCs, Centers, components and subordinate  
109 Command Collection Managers will also submit (b)(1) Sec 1.7(e) requirements through  
110 (b)(1) Sec 1.7(e) while keeping HQ informed. Refer to reference i.

111  
112 (c) (U) Users without (b)(1) Sec 1.7(e) can submit requirements by e-  
113 mail, message, or telecom to (b)(1) Sec 1.7(e)

114  
115 (2) (U) (b)(1) Sec 1.7(e)

116  
117 (a) (U) Provide timely, responsive processing and validation of  
118 USSTRATCOM Commander's, (b)(1) Sec 1.7(e)  
119 (b)(1) Sec 1.7(e)  
120 validation. (b)(1) Sec 1.7(e) execute  
121 requirements validation and tasking for time critical requirements and special  
122 circumstances after normal working hours and on weekends. Refer to  
123 reference e.

124  
125 (b) (U) Provide status to USSTRATCOM/J23 Intelligence Capabilities  
126 Branch of all Commander, USSTRATCOM, (b)(1) Sec 1.7(e) requirements.  
127 Assist in the coordination of (b)(1) Sec 1.7(e) requirements with other Unified  
128 Commands, National Agencies, and Services. Refer to reference e.

**SECRET**

39 collection requirements. NOTE: (b)(1) Sec 1.4(a) as  
40 outlined in reference b. and is not included in this appendix.

41  
42 a. (U) (b)(1) Sec 1.7(e) Refer to Annex B (Intelligence)

43  
44 b. (U) Friendly

45  
46 (1) (U) (b)(1) Sec 1.7(e) is responsible for  
47 (b)(1) Sec 1.7(e)  
48  
49 balancing competing priorities of military and national needs as detailed in  
50 reference b.

51  
52 (2) (U) (b)(1) Sec 1.7(e) and  
53 prioritizes collection requirements in line with the (b)(1) Sec 1.7(e)  
54 (b)(1) Sec 1.7(e)  
55  
56  
57

58  
59 (3) (U) (b)(1) Sec 1.7(e)  
60 will provide timely/responsive processing and validation of Commander,  
61 USSTRATCOM, (b)(1) Sec 1.7(e)  
62 (b)(1) Sec 1.7(e) Combatant Command  
63 intelligence requirements. (b)(1) Sec 1.7(e) requirements to the  
64 (b)(1) Sec 1.7(e) for validation. (b)(1) Sec 1.7(e)  
65 (b)(1) Sec 1.7(e)  
66  
67

68  
69 (4) (U) (b)(1) Sec 1.7(e) provide Commander,  
70 USSTRATCOM, and the Commanders of JFCCs with (b)(1) Sec 1.7(e)  
71 consultation, and support in planning activities.

72  
73 (5) (U) (b)(1) Sec 1.7(e)  
74 (b)(1) Sec 1.7(e) will conduct the (b)(1) Sec 1.7(e) support mission  
75 and provide (b)(1) Sec 1.7(e)  
76

77 c. (U) Assumptions. Refer to Base Plan.

78  
79 2. (U) Mission. Refer to Base Plan.

80  
81 3. (U) Execution. Refer to Annex B (Intelligence)

82  
83 a. (U) Concept of Operations

84

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AFB NE 68113-6500  
26 February 2008

1 APPENDIX 8 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)

2 (U) OPR: HQ USSTRATCOM/J2

3 (b)(1) Sec 1.7(e) (U)

4  
5 (U) References:

6  
7 a. (U) Intelligence Community Directive-1, Policy Directive for Intelligence  
8 Community Leadership, 1 May 2006 (U).

9  
10 b. (U) (b)(1) Sec 1.7(e) 22 Jul 05  
11 (S//TK).

12  
13 c. (U) (b)(1) Sec 1.7(e) (TS//SCI).

14  
15 d. (U) (b)(1) Sec 1.7(e) 18 February  
16 1997 (U).

17  
18 e. (U) (b)(1) Sec 1.7(e)  
19 (b)(1) Sec 1.7(e) 9 Feb 93 (U).

20  
21 f. (U) (b)(1) Sec 1.7(e)  
22 (b)(1) Sec 1.7(e) 1 December 2005 (U).

23  
24 g. (U) (b)(1) Sec 1.7(e)  
25 (b)(1) Sec 1.7(e) 9 June 2006 (S).

26  
27 h. (U) D-R-A-F-T Department of Defense Directive, SUBJECT: (b)(1) Sec 1.7(e)  
28 (b)(1) Sec 1.7(e) within the Department of Defense, Apr 05 (U).

29  
30 i. (U) Implementation Directive: Joint Functional Component for  
31 Intelligence, Surveillance, and Reconnaissance (JFCC ISR), 24 Jan 2005 (U).

32  
33 1. (S//REL USA, AUS, GBR) Situation. (b)(1) Sec 1.4(a)  
34 (b)(1) Sec 1.4(a)  
35 (b)(1) Sec 1.4(a) Given the current intelligence tasks in the  
36 (b)(1) Sec 1.4(a) to the overall  
37 plan. As such, this appendix provides a general overview of the (b)(1) Sec 1.4(a)  
38 organization, general responsibilities, and procedures for (b)(1) Sec 1.4(a)

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (e), and (g)~~  
~~Declassify on: 26 February 2032~~

**SECRET**

**SECRET**

129 (3) (U) USSTRATCOM JFCC ISR. Ensure proper national-level  
130 coordination and approval of appropriate (b)(1) Sec 1.7(e)  
131 support of this CONPLAN.

132  
133 c. (U) Coordinating Instructions. Refer to references.

134  
135 4. (U) Administration and Logistics

136  
137 a. (U) Logistics. Not applicable.

138  
139 b. (U) Reporting

140  
141 (1) (U) Originating Collection Management office will task appropriate  
142 processing and (b)(1) Sec 1.7(e) to satisfy validated USSTRATCOM  
143 requirements. (b)(1) Sec 1.7(e)

144  
145 (2) (S//REL) (b)(1) Sec 1.4(a)  
146 (b)(1) Sec 1.4(a)  
147  
148

149 5. (U) Command and Control. Refer to Annex B (Intelligence).

150  
151 a. Command Relationships. Refer to Annex B (Intelligence).

152  
153 b. Communications. Refer to Annex B (Intelligence).

154  
155  
156 Kevin P. Chilton  
157 General, USAF  
158 COMMANDER

159  
160  
161  
162  
163

**SECRET**

85 USSTRATCOM missions are or may be executed by, but not limited to, (b)(1) Sec 1.4(a)  
86 (b)(1) Sec 1.4(a)

87  
88 b. (U) Tasks

89  
90 (1) (U) USSTRATCOM Collection Managers

91  
92 (a) (U) USSTRATCOM/J2 Collection Managers submit (b)(1) Sec 1.7(e)  
93 (b)(1) Sec 1.7(e)

94 JWICS (ref c).

95  
96 (b) (U) USSTRATCOM JFCCs, Centers, components, and subordinate  
97 command Collection Managers will also submit (b)(1) Sec 1.7(e)  
98 (b)(1) Sec 1.7(e) while keeping HQ informed (ref i).

99  
100 (c) (U) Users without (b)(1) Sec 1.7(e)  
101 (b)(1) Sec 1.7(e) e-mail, message, or telecom to  
102 USSTRATCOM/J2 Collection Managers.

103  
104 (2) (U) (b)(1) Sec 1.7(e)

105  
106 (a) (U) Provide timely, responsive review and validation of  
107 USSTRATCOM (b)(1) Sec 1.7(e)  
108 (b)(1) Sec 1.7(e)

109  
110  
111 (b) (U) Provide status to USSTRATCOM/J2 of all Command (b)(1) Sec 1.7(e)  
112 (b)(1) Sec 1.7(e)

113  
114  
115  
116 (c) (U) Provide immediate information on and assessments of events  
117 that impact collection management tools, communications and dissemination  
118 systems, databases, collection sensor and systems, processing, and other  
119 support functions.

120  
121 (d) (U) Provide updates and status concerning changes that affect the  
122 execution of collection management functions. (b)(1) Sec 1.7(e)  
123 (b)(1) Sec 1.7(e) to facilitate the most responsive  
124 tasking of assets in support of the Commander, USSTRATCOM.

125  
126 (e) (U) (b)(1) Sec 1.7(e) assets in support of  
127 USSTRATCOM collection requirements.

128



SECRET

(b)(1) Sec 1.4(a)

40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84

a. (U) (b)(1) Sec 1.7 Refer to Annex B (Intelligence).

b. (U) Friendly

(1) (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

(2) (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

c. (U) Assumptions. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan.

3. (U) Execution. Refer to Annex B (Intelligence).

a. (U) Concept of Operations for (b)(1) Sec 1.7(e)  
Production

(1) (U) Collection Management. USSTRATCOM/J2 Intelligence Capabilities Branch will provide (b)(1) Sec 1.7(e) support to HQs staff elements only. USSTRATCOM JFCCs, Centers, components, and subordinate commands will assume (b)(1) Sec 1.7(e) for their organizations while keeping HQ informed. JFCC ISR will closely collaborate with USSTRATCOM/J2 to maintain awareness of requirements and ensure synchronization with DOD ISR. Ultimately, reporting agencies will be responsible to both the Command and its subordinate JFCCs.

(2) (S//REL) (b)(1) Sec 1.4(a) The DOD architecture for (b)(1) Sec 1.4(a) distributed throughout the DOD. (b)(1) Sec 1.4(a) required to support

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AFB NE 68113-6500  
28 February 2008

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39

APPENDIX 7 TO ANNEX B TO CDRUSSTRATCOM CONPLAN 8039 (U)

(U) OPR: HQ USSTRATCOM J2

(b)(1) Sec 1.7(e) (U)

(U) References:

a. (U) Joint Pub 2-01, Joint and National Intelligence Support to Military Operations, 7 October 2004 (U)."

b. (U) Chairman of the Joint Chiefs of Staff Instruction (CJCSI), (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) 28 January 2000 (TS).

c. (U) (b)(1) Sec 1.7(e) 18 February 1997 (U).

d. (U) (b)(1) Sec 1.7(e) 10 November 1996 (U)."

e. (U) (b)(1) Sec 1.7(e) 22 March 2007 (U)."

f (U) (b)(1) Sec 1.7(e)

1. (~~S~~//REL) Situation. Given the current intelligence tasks in the CONPLAN,

(b)(1) Sec 1.4(a)

Classified by: Multiple Sources  
Reason: 1.4(a), (c), and (g)  
Declassify on: 26 February 2032

**SECRET**

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
26 February 2008

1 ANNEX J TO COMMANDER USSTRATCOM CONPLAN 8039 (U)  
2 (U) OPR: HQUSSTRATCOM/J53  
3 COMMAND RELATIONSHIPS (U)

4 References:

5 a. (U) Unified Command Plan (UCP), 5 May 06 (U//FOUO)

6 b. (U) (b)(1) Sec 1.7(e) 1 Sep 06 (TS)

7 c. (U) Joint Publication 1-02, Department of Defense Dictionary of  
8 Military and Associated Terms, 12 April 2001 (As Amended Through 20 March  
9 2006) (U)

10 d. (U) Joint Pub 1, Doctrine for the Armed Forces of the United States,  
11 14 May 2007 (U)

12 e. (U) Delegation of Disclosure Authority Letter, National Disclosure  
13 Policy Committee Case No. 6005-00 - Multiple Countries, 7 Jun 00 (S)

14 f. (U) Memorandum of Arrangement between The Department of  
15 Defence of Australia, The Ministry of Defence of The United Kingdom of Great  
16 Britain and Northern Ireland, and The Department Of Defense of The United  
17 States of America on Information Operations Data Exchange, 6 May 03 (U)

18 g. (U) 2004 National Response Plan (NRP), Cyber Annex, Dec 04 (U)

19 h. (U) Trilateral Memorandum of Agreement among the Department of  
20 Defense, the Justice Department and the Intelligence Community Regarding

21 (b)(1) Sec 1.7(e)

22 (b)(1) Sec 1.7(e) 9 May 07 (S//NFS//NF)

23 1. (U) General

24 a. (U) Operational Area(s). Refer to Base Plan para 1.b.

25 b. (U) Scope. This Annex defines the command and cooperative  
26 relationships between USSTRATCOM, DOD organizations, non-DOD USG  
27 agencies, and civilian entities as they pertain to cyberspace operations.

~~Classified by: Multiple Sources~~

~~Reason: 1.4(a), (e), and (g)~~

~~Declassify on: 26 February 2033~~

**SECRET**

**SECRET**

28 2. (~~S//REL USA, AUS, GBR~~) Mission. CDRUSSTRATCOM plans and directs  
29 integrated DOD cyber operations (b)(1) Sec 1.4(a)

30 (b)(1) Sec 1.4(a)

31 defend the DOD networks from aggression, and as directed, use cyberspace to  
32 advance and defend US interests.

33 3. (U) Execution. CDRUSSTRATCOM will plan and carry out the strategic,  
34 global cyberspace missions for DOD. CDRUSSTRATCOM will be designated as  
35 the supported commander by the POTUS or SECDEF, and CJCS for strategic,  
36 global Cyberspace Operations (CO) and as a supporting commander for  
37 geographic regional CO. As the DOD military lead for CO, CDRUSSTRATCOM  
38 serves as a conduit to the C/S/As for operational policy issues and mission  
39 operations.

40 a. (U) CDRUSSTRATCOM Responsibilities

41 (1) (U) Coordinate through the USSTRATCOM Director, Global  
42 Operations/J3 all CO support requested by C/S/As.

43 (a) (U) Act as C/S/A's primary contact for cyber support through  
44 the USSTRATCOM/J3 via the Global Operations Center (GOC). C/S/As can  
45 also request cyber support through any STRATCOM component. Such  
46 requests will in turn be forwarded to the GOC for internal coordination/action.

47 (b) (U) Designate the USSTRATCOM Director, Plans and Policy/J5  
48 as the staff element responsible for consolidating, prioritizing, deconflicting and  
49 assigning USSTRATCOM Cyberspace resources based on commander's  
50 guidance.

51 (c) (U) Retain Administrative Control (ADCON) authority of the  
52 deployed USSTRATCOM CO components (teams consisting of HQ  
53 USSTRATCOM, JFCC NW, JTF GNO, and JIOWC personnel, depending on  
54 mission requirements) as appropriate.

55 (2) (U) Exercise Coordinating Authority (CA) with C/S/As, as defined  
56 by reference (d) above.

57 (3) (U) Develop relationships with the C/S/As and external  
58 organizations that will maintain and augment existing HQ USSTRATCOM, JTF  
59 GNO, JFCC NW, JFCC GSI, JFCC SPACE, and JIOWC relationships.

60 (4) (U) Coordinate (b)(1) Sec 1.7(e)  
61 as appropriate.

62 (5) (U) Evaluate, select/pursue cyber threats, plan, and prioritize the  
63 desired effects necessary to achieve the appropriate combination of the plan's  
64 (b)(1) Sec 1.7(e) based on the scenario.

**SECRET**

**SECRET**

65 b. (U) USSTRATCOM Components

66 (1) (U) Lead Component and assignment of forces.

67 (U)(a) CDRUSSTRATCOM designates JTF GNO as the lead component  
68 to operate and defend the DOD GIG. All other USSTRATCOM components are  
69 assigned in a supporting role for the operation and defense of the DOD GIG.

70 (b) (~~S//REL USA, AUS, GBR~~) CDRUSSTRATCOM will conduct  
71 military operations in cyberspace as either the supported or supporting  
72 commander. CONPLAN 8039 will provide the methodology for determining  
73 (b)(1) Sec 1.4(a) CDRUSSTRATCOM will  
74 designate a lead component and assign forces for execution of specified  
75 cyberspace missions based upon the nature of the crisis/contingency. The  
76 lead component has the responsibility to integrate offensive and defensive  
77 activities (see Figure 1). For timing and tempo of operations, USSTRATCOM  
78 assigned cyber forces will (b)(1) Sec 1.4(a)  
79 (b)(1) Sec 1.4(a) The USSTRATCOM designated lead component:

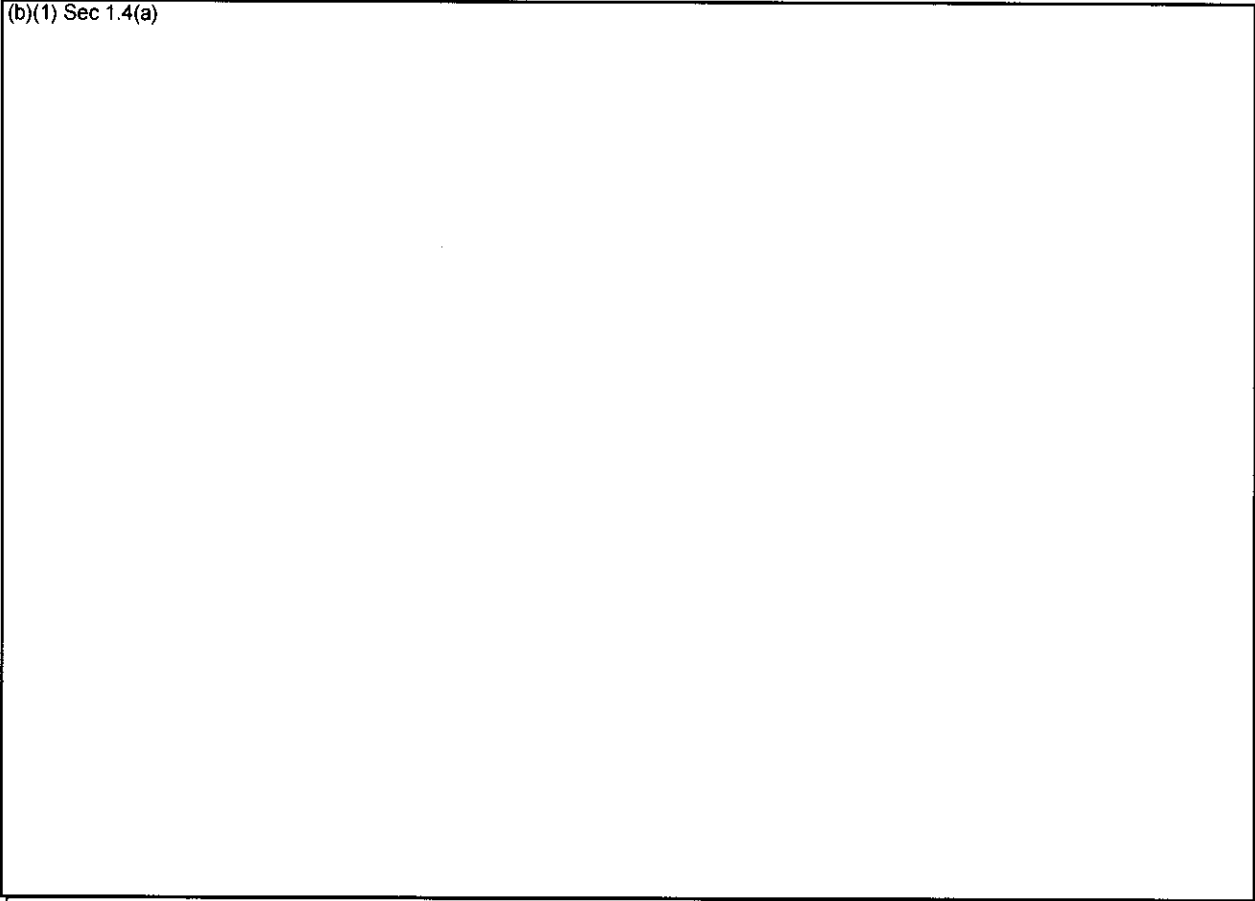
80 1 (~~S//REL USA, AUS, GBR~~) Will be delegated (b)(1) Sec 1.4(a)  
81 (b)(1) Sec 1.4(a) day-to-  
82 day management of assigned cyberspace forces in executing the assigned  
83 mission, as appropriate.

84 (U)2 (~~S//REL USA, AUS, GBR~~) Will support theater operations as  
85 directed by CDRUSSTRATCOM.

86 (U)3 (~~S//REL USA, AUS, GBR~~) Will collaborate and coordinate  
87 across the USSTRATCOM staff, Service component staffs assigned to  
88 USSTRATCOM and their respective operations centers, Combatant  
89 Commanders, and other DOD and non-DOD partners to ensure unity of effort  
90 in support of military and other national security operations.

91 4 (~~S//REL USA, AUS, GBR~~) Will request to establish (b)(1) Sec 1.4(a)  
92 (b)(1) Sec 1.4(a) to plan, synchronize,  
93 collaborate and deconflict operations.

(b)(1) Sec 1.4(a)

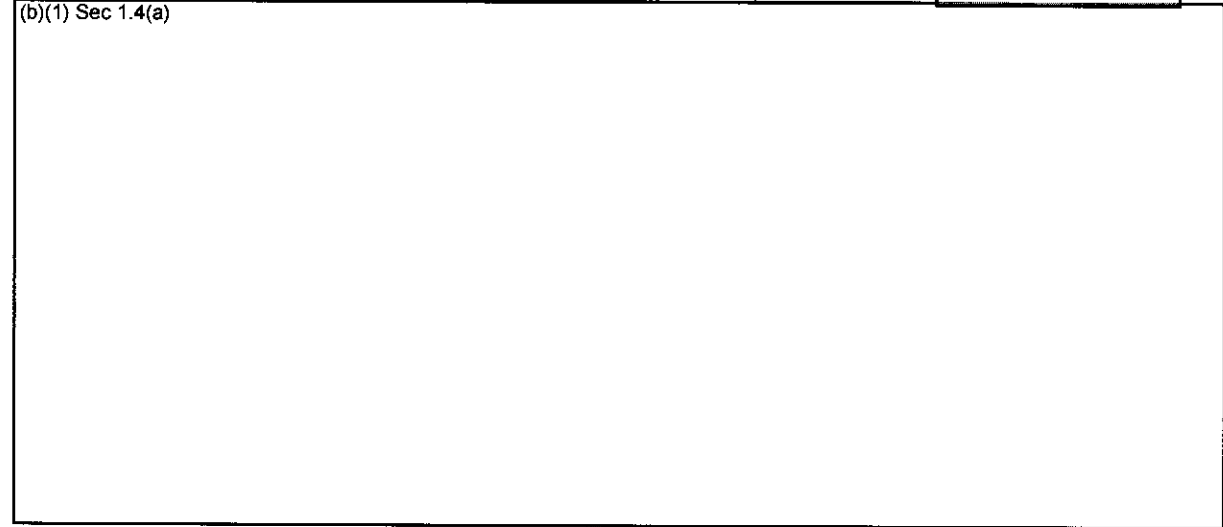


(U) Figure 1 Command Structure (S//REL USA, AUS, GBR)

94 (c) (~~S//REL USA, AUS, GBR~~) Assignment of forces. In general, the  
95 following principles apply to the assignment of cyber forces: (b)(1) Sec 1.4(a)

96 (b)(1) Sec 1.4(a)

97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109



110

(2) (U) USSTRATCOM Components and Service Components

**SECRET**

111 (a) (U) USSTRATCOM Components

112 1 (U//~~FOUO~~) JTF GNO. As directed by CDRUSSTRATCOM,  
113 JTF GNO supports the USSTRATCOM-assigned Unified Command Plan (UCP)  
114 mission of global network operations. The UCP 2006 states that USSTRATCOM  
115 shall be responsible for planning, integrating, and coordinating DOD global  
116 network operations by directing GIG operations and defense and identifying  
117 and advocating these desired characteristics and capabilities.  
118 CDRUSSTRATCOM, through CDR, JTF GNO, provides the DOD with the  
119 direction and oversight to operate and defend the GIG and accommodate  
120 interfaces to coalition, allied and non-DOD users and systems. CDR, JTF GNO  
121 reports directly to CDRUSSTRATCOM and exercises TACON / OPCON of  
122 assigned forces. JTF GNO, upon implementation of CONPLAN 8039 and on  
123 behalf of CDRUSSTRATCOM, will assume TACON of assigned defensive CO  
124 forces. Commander JTF GNO executes NetOps via assigned forces. As  
125 required to fulfill mission requirements, CDR JTF-GNO has authority for direct  
126 liaison (DIRLAUTH) with other DOD components to include C/S/As to  
127 exchange information germane to cyberspace activities and promote situational  
128 awareness relative to hostile acts directed toward DOD networks. The following  
129 specific authorities are granted to CDR, JTF GNO:

130 a (U//~~FOUO~~) CA for the planning and execution of the GIG  
131 NetOps mission.

132 b (U//~~FOUO~~) OPCON or TACON of assigned NetOps and  
133 CND forces, as directed.

134 c (U//~~FOUO~~) Direct Liaison Authorized (DIRLAUTH)  
135 between JTF GNO and the following: USSTRATCOM functional components,  
136 Service components, subordinate organizations, Combat Commands, and  
137 communities of interest; USSTRATCOM will be kept informed. CDR, JTF GNO,  
138 is encouraged, consistent with DOD rules and regulations, to develop robust  
139 coordinating relationships for information sharing to include: non-DOD US  
140 government organizations, intergovernmental organizations, nongovernmental  
141 organizations, multinational military commands (alliances and coalitions), state  
142 and local governments, commercial and research communities.

143 2 (U) JFCC NW. On a daily basis, JFCC NW will conduct  
144 operational and tactical level planning and day-to-day employment of assigned  
145 and attached forces, integration of (b)(1) Sec 1.7(e)  
146 (b)(1) Sec 1.7(e)  
147 effects or that directly support national objectives in and through cyberspace.  
148 This includes (b)(1) Sec 1.7(e)  
149 (b)(1) Sec 1.7(e) in support of other Combatant Commanders,  
150 as directed. At a minimum, the JFCC NW is required to:

**SECRET**

151                    a (U) Synchronize all capabilities for operations in and  
152 through cyberspace with the JTF GNO, JIOWC, and other JFCCs, as  
153 necessary. Assume OPCON or TACON, where applicable, of cyber forces for  
154 day-to-day and crisis operations.

155                    b (U) Develop recommendations to alleviate, from a global  
156 perspective, operational resource conflicts for operations capabilities of cyber  
157 forces.

158                    c (U) Develop Course of Action (COA) recommendations for  
159 operations in and through cyberspace in support of USSTRATCOM and  
160 national strategic objectives. Support JFCC GSI for the integration of  
161 operations in and through cyberspace into USSTRATCOM global strike COAs.  
162 Provide an embedded capability in the Global Operations Center (GOC) to  
163 support JFCC GSI mission of operational level integration of USSTRATCOM  
164 missions and maintaining situational awareness for the commander.

165                    d (U) Coordinate and maintain tactical level intelligence, as  
166 necessary, to support components of operations in and through cyberspace.

167 Provide all (b)(1) Sec 1.7(e)  
168 (b)(1) Sec 1.7(e)  
169

170                    e (U) Establish a relationship with mission area experts in  
171 the applicable regional commander's Standing Joint Force Headquarters  
172 (SJFHQ) to provide operational support for NW capabilities. This relationship  
173 will include the training and periodic qualification of NW support in SJFHQs,  
174 as required.

175                    f (U) Provide support for headquarters USSTRATCOM and  
176 other geographic and functional Combatant Commanders exercise, wargames,  
177 and experimentation requirements. Integrate and synchronize efforts with  
178 USSTRATCOM Training and Exercise Division (J37). Support headquarters  
179 development of military utility assessments, research and development efforts,  
180 and advocacy of capability needs for the Joint Capabilities Integration  
181 Development System (JCIDS) process.

182                    g (U) Report operational readiness assessment of assigned  
183 mission areas, as directed by headquarters.

184                    h (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
185 (b)(1) Sec 1.4(a) CDR USSTRATCOM or the requesting CCDR.

186                    (1) (~~S//REL USA, AUS, GBR~~) Authority necessary to  
187 (b)(1) Sec 1.4(a)  
188



**SECRET**

189  
190

(b)(1) Sec 1.4(a)

191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204

(2) (S//REL USA, AUS, GBR) The following are

(b)(1) Sec 1.4(a)

operations (see Table 4). Subject (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

205  
206  
207  
208

Table 1 (b)(1) Sec 1.4(a) (S//REL USA, AUS, GBR)

(a) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

**SECRET**

209 (1) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
210 (b)(1) Sec 1.4(a)  
211  
212  
213

214 (2) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
215 (b)(1) Sec 1.4(a)  
216  
217  
218

219 (3) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
220 (b)(1) Sec 1.4(a) computers, networks, information and information systems is  
221 authorized only for the purpose of conducting an approved operation as defined  
222 in this plan. (b)(1) Sec 1.4(a)  
223 (b)(1) Sec 1.4(a)

224 (4) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
225 (b)(1) Sec 1.4(a)  
226  
227  
228  
229  
230

231 (5) (S//REL USA, AUS, GBR) Supported  
232 JFC notification is required for (b)(1) Sec 1.4(a)  
233 (b)(1) Sec 1.4(a) CDRUSSTRATCOM may delegate this  
234 authority to the CDR JFCC NW when acting as supported commander. (b)(1) Sec 1.4(a)  
235 (b)(1) Sec 1.4(a)  
236

237 (6) (S//REL USA, AUS, GBR) Supported  
238 JFC approval is required for (b)(1) Sec 1.4(a)  
239 (b)(1) Sec 1.4(a)  
240 (b)(1) Sec 1.4(a) CDRUSSTRATCOM may delegate this authority  
241 to the CDR JFCC NW when acting as supported commander, which may be  
242 further delegated to a General Officer/Flag Officer within JFCC NW. (b)(1) Sec 1.4(a)  
243 (b)(1) Sec 1.4(a)  
244

245 (7) (S//REL USA, AUS, GBR) All formal  
246 requests for approval (b)(1) Sec 1.4(a)  
247 (b)(1) Sec 1.4(a)

**SECRET**

**SECRET**

248  
249  
  
250  
251  
252  
253  
254  
255  
256

(b)(1) Sec 1.4(a)

(b) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

257  
258

i (U) The CDR JFCC NW is assigned the following authorities:

259  
260

(1) (U) CA for the planning and execution of the CO mission.

261  
262

(2) (U) OPCON or TACON of assigned cyberspace forces, as directed by headquarters.

263  
264  
265  
266  
267  
268

(3) (U) DIRLAUTH between JFCC NW and other joint and Service components, Combatant Commanders, and DOD agencies, while keeping headquarters informed. JFCC Commanders are encouraged, consistent with DOD rules and regulations, to develop the robust coordinating relationships, to include inter-agency and combined forces where required, to enhance the mission effectiveness of operations in and through cyberspace.

269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281

3 (U//~~FOUO~~) JFCC GSI. JFCC GSI will act as the overall lead USSTRATCOM component in direct support of the CDRUSSTRATCOM to develop integrated crisis response COAs, provide integrated analysis of the Command's global mission capabilities, provide execution recommendations for supported and supporting mission tasks, execute global strike missions when directed, and, through a JFCC GSI managed GOC that integrates inputs of all components and Service task forces, provide the headquarters with situational awareness for all operational responsibilities. Provide continuous situational awareness of assigned forces engaged in ongoing global strike operations. Provide coordinated tasking from the headquarters to other joint components and Service task forces, as necessary, for the synchronization of all USSTRATCOM operational and tactical mission planning and execution needs IAW USTRATCOM HC2I CONOPS. At a minimum, the JFCC GSI is required to:

282  
283  
284  
285

a (U//~~FOUO~~) In accordance with USSTRATCOM's Intelligence Integration CONOPS, coordinate with the (b)(1) Sec 1.7(e) (b)(1) Sec 1.7(e) global strike intelligence requirements.

**SECRET**

286                    b (U//~~FOUO~~) Support USSTRATCOM led efforts to create  
287 and maintain strategic-level OPLANs. Support development and coordination of  
288 OPLANs and CONPLANs, as directed by headquarters. Support other  
289 Combatant Commands with global strike operational planning and execution,  
290 as directed by headquarters.

291                    c (U//~~FOUO~~) Assume OPCON or TACON of (b)(1) Sec 1.7(e)  
292 (b)(1) Sec 1.7(e) as directed.

293                    d (U//~~FOUO~~) Support HQ coordination with geographic  
294 and functional Combatant Commanders to support ongoing and future  
295 operational requirements for USSTRATCOM global strike capabilities.

296                    e (U//~~FOUO~~) Provide support for HQ USSTRATCOM and  
297 other geographic and functional Combatant Commanders' exercise, war game  
298 and experimentation requirements. Integrate and synchronize efforts with  
299 USSTRATCOM Training and Exercise Directorate (J7).

300                    f (U//~~FOUO~~) Support headquarters development of global  
301 strike mission research and development and advocacy of capability needs for  
302 the Joint Capabilities Integration and Development System (JCIDS) process.

303                    g (U//~~FOUO~~) Be the central manager of the (b)(1) Sec 1.7(e)  
304 (b)(1) Sec 1.7(e) capability.

305                    h (U//~~FOUO~~) Manage the GOC.

306                    i (U//~~FOUO~~) Chair the Information Operations Working  
307 Group (IOWG).

308                    j (U//~~FOUO~~) Manage the Joint Integration Working Group  
309 (JIWG).

310                    k (U//~~FOUO~~) Manage the Joint Planning Working Group  
311 (JPWG).

312                    4 (U) JIOWC. JIOWC is responsible for planning, integrating  
313 and coordinating the IO core capabilities of (b)(1) Sec 1.7(e) OPSEC and (b)(1) Sec 1.7(e) and  
314 (b)(1) Sec 1.7(e) in support of JFCs. JIOWC is also the USSTRATCOM lead  
315 for strengthening IO capabilities across the DOD and is responsible for  
316 supporting the SC planning efforts of STRATCOM missions and JFCs when  
317 requested. At a minimum, the JIOWC is required to:

318                    a (U) Enable JFCs to plan and execute IO, (b)(1) Sec 1.7(e)  
319 (b)(1) Sec 1.7(e) OPSEC, (b)(1) Sec 1.7(e)  
320 and CNO.

**SECRET**

**SECRET**

321 b (U) Interface with the Joint Staff, Military Services, DOD  
322 and non-DOD agencies to coordinate and integrate IO efforts for joint  
323 commanders.

324 c (U) Participate in (b)(1) Sec 1.7(e)  
325 (b)(1) Sec 1.7(e) support to Combatant Commanders.

326 d (U) Provide assistance to JFC IO intelligence support  
327 efforts.

328 e (U) Evaluate IO effectiveness in military operations.

329 f (U) Provide Joint IO wargaming simulations to support  
330 joint exercises and experimentation.

331 g (U) Assist with strategic IO planning and theater  
332 engagement.

333 h (U) The Commander, JIOWC will deploy task organized IO  
334 support teams to assist C/S/As as directed by CDRUSSTRATCOM.

335 i (U) Upon SecDef approval, the Chief, JIOWC Combatant  
336 Commander Support Team will fall under OPCON authority of the supported  
337 commander.

338 5 (U) JFCC SPACE. JFCC SPACE will optimize planning,  
339 execution, and force management of the assigned missions and to coordinate  
340 space operations. JFCC SPACE supports CDRUSSTRATCOM in the conduct of  
341 space operations and exercises OPCON of designated space and missile-  
342 warning forces on behalf of CDRUSSTRATCOM. CDR JFCC SPACE is  
343 designated as the Global Space Coordinating Authority (GSCA) and the lead  
344 USSTRATCOM component for execution of Defensive Space Control (DSC)  
345 which includes the satellite Telemetry, Tracking & Control (TTC)-portion of  
346 cyberspace.

347 6 (U) JFCC IMD. JFCC IMD serves as the CA on behalf of  
348 CDRUSSTRATCOM for planning and execution of the IMD mission. JFCC IMD  
349 develops and coordinates IMD concepts of operations and supporting  
350 operational plans, to include OPLANs, CONPLANs, FUNCPLANs, and  
351 SUPPLANs, as directed by HQ USSTRATCOM. JFCC IMD assumes OPCON or  
352 TACON control, as directed, of designated IMD capabilities for day-to-day and  
353 crisis operations. JFCC IMD provides day-to-day and crisis operational  
354 support to missile defense components. JFCC IMD provides an embedded  
355 capability in the GOC to support the JFCC GSI tasks of operational level  
356 integration of USSTRATCOM missions and maintaining situational awareness  
357 for the commander.

**SECRET**

**SECRET**

358 7 (U) JFCC ISR. JFCC ISR conducts planning to employ DOD  
359 ISR resources to meet Combatant Commander, national, and departmental  
360 requirements. (b)(1) Sec 1.7(e)

361 (b)(1) Sec 1.7(e)  
362

363 the Joint Staff, U.S. Joint Forces Command (USJFCOM), Combatant  
364 Commanders, the military Services, and other mission partners, JFCC ISR  
365 ensures the integration of DOD and national ISR efforts to satisfy Combatant  
366 Commander and national operational and intelligence requirements. JFCC ISR  
367 planning synchronizes the use of national, DOD, and, when feasible,  
368 Allied/Coalition ISR capabilities with employment of theater ISR resources.

369 (b) (U) USSTRATCOM Service Components

370 1 (~~S//REL USA, AUS, GBR~~) U.S. Army Forces. USSTRATCOM  
371 has COCOM of SMDC/ARSTRAT. (b)(1) Sec 1.4(a)

372 (b)(1) Sec 1.4(a)  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384

385 2 (U) U.S. Naval Forces.

386 a. The Navy (b)(1) Sec 1.7(e)

387 (b)(1) Sec 1.7(e) Navy forces certified for network defense are  
388 embedded in the parent force structure of all Navy component commanders  
389 assigned by their respective commanders with assignment of additional forces  
390 via Naval Component Task Force-ND (NCTF-ND) as required. JTF GNO has  
391 TACON authority of the NCTF-ND (for cyber defense only). The Navy Global  
392 Operations and Security Center (NAVGNOSEC) is OPCON to JTF GNO. In  
393 response to network events or activities, as determined by CDR USSTRATCOM  
394 or CDR JTF GNO, the Navy Cyber Defense Operations Command (NCDOC)  
395 shall instantaneously be attached to CDR JTF GNO, who will exercise TACON  
396 upon contact with the NCDOC until such time that the responses to the events  
397 or activities are declared complete by CDR JTF GNO, at which time the Navy  
398 will resume control of the NCDOC. (b)(1) Sec 1.7(e)

399 (b)(1) Sec 1.7(e) When directed

**SECRET**

400 by a Joint Staff deployment order, (b)(1) Sec 1.7(e)

401 (b)(1) Sec 1.7(e)

402

403

404

405 CDRUSSTRATCOM is designated the supported commander.

406 b. The Marine Corps (b)(1) Sec 1.7(e)

407 (b)(1) Sec 1.7(e) Marine forces certified for

408 network defense are embedded in the parent force structure of all Marine

409 component commanders with assignment of additional forces via as required.

410 The Marine Corps Network Operations and Security Center (MCNOSC) is

411 OPCON to JTF GNO for CND. Assignment of other Marine forces will be

412 coordinated through MARFORSTRAT.

413 3 (S//REL USA, AUS, GBR) U.S. Air Force Forces.

414 USSTRATCOM has COCOM of 8 AF (b)(1) Sec 1.4(a)

415 (b)(1) Sec 1.4(a)

416

417

418

419

420

421

422

423 c. (U) (b)(1) Sec 1.7(e)

424 (1) (C//REL) (b)(1) Sec 1.4(a)

425 (b)(1) Sec 1.4(a)

426

427

428

429

430

431

432

433

434

435 (2) (U) (b)(1) Sec 1.7(e)

436 (b)(1) Sec 1.7(e)

437

438

439

440 protection (See Base Plan) up to the Top Secret level for the goal of

**SECRET**

441 strengthening information networks; to improve the confidentiality, integrity  
442 and availability of information systems; and improve the prediction, detection  
443 and response capabilities. USSTRATCOM/J51 is designated as the United  
444 States National Lead; JTF GNO is responsible for the operational mission.

445 d. (U) Alternate Procedures (Succession to Command)

446 (a) (U) When the position of the combatant commander is vacant,  
447 or in the temporary absence or disability of the combatant commander, the  
448 deputy commander acts as the combatant commander and performs the duties  
449 of the combatant commander until a successor is appointed or the absence or  
450 disability ceases. If a deputy commander has not been designated, or is also  
451 temporarily absent or disabled, interim command shall pass to the next senior  
452 officer present for duty eligible to exercise command, regardless of Service  
453 affiliation.

454 (c) (U) In the event JTF GNO cannot execute command of JTF GNO  
455 due to lack of communications or other reasons, succession of command is  
456 Deputy JTF GNO, Commander Marine Forces (COMMARFOR), Commander Air  
457 Force Forces (COMAFFOR), Commander Global Network Operations and  
458 Security Center (CDR GNOSC), Naval Network Warfare Command  
459 (NAVNETWARCOM) and Commander Army Forces (COMARFOR).

460 (b) (U) In the event CDR JFCC NW cannot execute command of  
461 JFCC NW due to lack of communications or other reasons, succession of  
462 command is Deputy JFCC NW.

463 (d) (U) In the event CDR JIOWC cannot execute command of  
464 JIOWC due to lack of communications or other reasons, succession of  
465 command is Deputy JIOWC.

466 4. (U) Support and Coordination Relationships

467 (U) a. (~~S//REL USA, AUS, GBR~~) Supporting Military Forces

468 (1) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
469 (b)(1) Sec 1.4(a)  
470  
471 (b)(1) Sec 1.4(a) USSTRATCOM or  
472 the supported regional commander.

473 (2) (U) USSTRATCOM Combatant Commander Liaison. USSTRATCOM  
474 Liaison Officers (LNOs) will assist COCOM's in coordinating USSTRATCOM  
475 cyberspace activities within specific geographic AORs.

**SECRET**



**SECRET**

476 (a) (U) All cyber forces supporting a CDR USSTRATCOM mission will  
477 immediately establish liaison with the USSTRATCOM LNO when arriving in a  
478 commander's theater.

479 (b) (U) USSTRATCOM regional LNOs will assist coordination of  
480 USSTRATCOM CO activities between USSTRATCOM and the GCCs.

481 b. Coordinating Authorities (Integration)

482 (1) (U) JFCC GSI

483 (U) (a) (~~S//REL USA, AUS, GBR~~) Coordinate requirements of the lead  
484 Component for non-routine/-daily activities, functions and objectives.

485 (b) (~~S//REL USA, AUS, GBR~~) In coordination w/ JTF GNO, JFCC  
486 NW, JIOWC & JFCC SPACE, (b)(1) Sec 1.4(a)  
487 (b)(1) Sec 1.4(a) DOD cyberspace.

488 (c) (~~S//REL USA, AUS, GBR~~) Assist JIOWC in the development of  
489 (b)(1) Sec 1.4(a)  
490 operations in and through cyberspace.

491 (d) (~~S//REL USA, AUS, GBR~~) In coordination with JTF GNO, JFCC  
492 NW, JIOWC and JFCC SPACE, (b)(1) Sec 1.4(a)  
493 (b)(1) Sec 1.4(a) to facilitate  
494 USSTRATCOM cyber execution when in the supporting role.

495 (U) (e) (~~S//REL USA, AUS, GBR~~) Provide initial assessments of  
496 operations, lessons learned, shortfalls and additional requirements or  
497 authorities as required.

498 (U)(2) (~~S//REL USA, AUS, GBR~~) HOUSTRATCOM/J3. Assist in the  
499 coordination and deconfliction with GCCs in support of CONPLAN 8039,  
500 Cyberspace Operations.

501 c. Supporting Agencies

502 (1) (U) The National Cyber Response Coordination Group (NCRCG).  
503 JTF GNO supports and coordinates with the National Cyber Response  
504 Coordination Group (NCRCG) on behalf of USSTRATCOM. Per ref g, the  
505 NCRCG is an interagency forum where organizations responsible for a range of  
506 activities (technical response and recovery, law enforcement, intelligence, and  
507 defensive measures) coordinate for the purposes of preparing for and executing  
508 an efficient and effective response to a cyber incident of national significance.

509 (2) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
510 (b)(1) Sec 1.4(a) CDRUSSTRATCOM for DOD

**SECRET**

511 computers and DOD computer networks of the GIG. (b)(1) Sec 1.4(a)

512 (b)(1) Sec 1.4(a)

513

514

515 (3) (U) Joint Warfare Analysis Center (JWAC). The JWAC provides

516 (b)(1) Sec 1.7(e)

517

518

519

520 this CONPLAN, all JWAC support for operations in and through cyberspace  
521 should be coordinated through USSTRATCOM/J3. When this CONPLAN is not  
522 in effect, direct liaison (per C/S/A policy) is customary.

523 (4) (U) National Infrastructure Protection Center (NIPC). The NIPC  
524 serves as the focal point for threat assessment, warning, investigation, and  
525 response to threats or attacks against national critical information  
526 infrastructures. It serves as both a national security and law enforcement  
527 organization to detect, deter, assess, warn of, respond to, and investigate  
528 computer attacks, intrusion and unlawful acts target against the GIG.  
529 USSTRATCOM will normally interface with the NIPC through JTF GNO.

530 (5) (U) (b)(1) Sec 1.7(e)

531 (b)(1) Sec 1.7(e)

532

533

534

535

536

537 (6) (U) (b)(1) Sec 1.7(e)

538 (b)(1) Sec 1.7(e)

539

540

541

542

543 (7) (U) (b)(1) Sec 1.7(e)

544 (b)(1) Sec 1.7(e)

545

546

547

548 d. Coordination With Diplomatic Agencies

549 (1) (U) Department of State (DOS). The SECDEF will coordinate with  
550 the Secretary of State on matters concerning diplomatic relations with foreign

**SECRET**

551 governments involved in cyberspace operational matters. Under normal  
552 circumstances, CDRUSSTRATCOM will coordinate with the CJCS who in turn  
553 will coordinate with the DOS, when considering or recommending (b)(1) Sec 1.7(e)  
554 (b)(1) Sec 1.7(e) as a cyberspace COA.

555 (2) (U) Department of Commerce (DOC). The SECDEF will coordinate  
556 with the Secretary of Commerce on matters concerning interstate and  
557 international commerce. There are three main areas of interest related to DOC  
558 federal regulatory responsibility concerning computer systems and computer  
559 networks: 1) regulating foreign sales of such technology, 2) the National  
560 Bureau of Standards that establishes standards and protocols for such  
561 technology, and 3) regulating interstate and international commerce related to  
562 such technology. Under normal circumstances, CDRUSSTRATCOM will  
563 coordinate with the CJCS who will coordinate with the DOC, on matters  
564 involving the DOD GIG.

565 5. Command and Control. (Command Posts).

566 a. (~~S//REL USA, AUS, GBR~~) Global Operation Center (GOC). The GOC

567 (b)(1) Sec 1.4(a)  
568  
569  
570

571 b. (U) JTF GNO

572 (1) (U) The Global NetOps Center (GNC) is the JTF GNO Command  
573 Center responsible for executing the daily operation and defense of the GIG.  
574 The GNC provides the overall management, control, and technical direction for  
575 GIG NetOps and oversees a collaborative coordination process involving all  
576 C/S/As, supporting the business, intelligence and warfighting needs of POTUS,  
577 SECDEF and the NetOps Community

578 (2) (U) JTF GNO has a full-time LE/CI Center for coordinating LE/CI  
579 activities in support of cyberspace missions. DOD LE/CI organizations have  
580 assigned full or part-time LE/CI agents from each of the LE/CI agencies,  
581 including Naval Criminal Investigative Service (NCIS), Defense Criminal  
582 Investigative Service (DCIS), Air Force Office of Special Investigations (OSI), US  
583 Army Criminal Investigations Division (USACID) and Army Intelligence and  
584 Security Command (INSCOM). JTF GNO LE/CI Center maintains a  
585 coordinating relationship with the IAIP, DHS.

586 c. (U) JFCC NW. JFCC NW (b)(1) Sec 1.7(e)  
587 (b)(1) Sec 1.7(e)

~~SECRET~~

588 d. (U) JIOWC. The JIOWC is located at Lackland AFB in San Antonio  
589 Texas. The organization provides full spectrum IO planning support to C / S /  
590 | A's worldwide through COCOM support teams.

591

592

593

594 | Kevin P. Chilton  
595 General, USAF  
596 Commander

597

598

599 Official:  
600 Mark H. Owen  
601 Brigadier General, USAF  
602 USSTRATCOM Plans and Policy

~~SECRET~~

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
26 February 2008

1 ANNEX K TO USSTRATCOM CONPLAN 8039 (U)

2 (U) OPR: HQ USSTRATCOM J675

3 COMMAND, CONTROL, COMMUNICATIONS AND COMPUTER (C4) SYSTEMS  
4 (U)

5 (U) References:

6 a. (U) USSTRATCOM Strategic Administrative Instruction (SAI) 301-6,  
7 Collateral Automated Information System (AIS) Security Policy, Current Edition  
8 (U)

9 b. (U) USSTRATCOM Strategic Administrative Instruction (SAI) 500-1,  
10 Information Operations, Current Edition (U)

11 c. (U) (b)(1) Sec 1.7(e)

12 (b)(1) Sec 1.7(e)

13  
14 d. (U) Chairman of the Joint Chiefs of Staff Operation Order (CJCS OPORD)  
15 2-FY, Survivable Mobile Command Center Operations (S)

16 e. (U) CJCSI 6510.01D, Information Assurance and Computer Network  
17 Defense, Current Edition (U)

18 f. (U) CJCSI 3320.01B, "Electromagnetic Spectrum Use in Joint Military  
19 Operations", 15 May 06 (U)

20 g. (U) CJCSI 3320.02B-1, "Joint Spectrum Interference Resolution (JSIR),"  
21 27 Jan 06 (S)

22 h. (U) CJCSM 3320.02C, "Joint Spectrum Interference Resolution (JSIR),"  
23 27 Jan 06 (U)

24

25

26

27 ~~Classified by: Multiple Sources~~

28 ~~Reason: 1.4(a), (c), and (g)~~

29 ~~Declassify on: 26 February 2033~~

30

31

32

**SECRET**

**SECRET**

33 1. (U) Situation

34 a. (U) (b)(1) Sec 1.7(e) (See Annex B, (b)(1) Sec 1.7(e))

35 b. (U) Friendly. See Appendix J.

36 (1) (U) Command Centers. See Appendix J.

37 (2) (U) (b)(7)(E) Provides  
38 (b)(7)(E)  
39  
40  
41

42 (a) (U) Systems Experts: (b)(7)(E)

43 (b) (U) Network Management and Payload Control:  
44 (b)(7)(E)

45 (c) (U) (b)(7)(E)  
46 (b)(7)(E)

47 (d) (U) Focal Point for implementation of Commander (b)(7)(E)  
48 requirements: (b)(7)(E)  
49 (b)(7)(E)

50 (3) (U) (b)(7)(E)  
51 (b)(7)(E)  
52  
53

54 (a) (U) System Expert: (b)(7)(E)

55 (b) (U) Network Management and Payload Control:  
56 (b)(7)(E)

57 (c) (U) (b)(7)(E)

58 (d) (U) Focal Point for Unified Commander: SMC for authorized  
59 networks; Unified Commander communications planners for requirements.

60 (4) (U) (b)(7)(E)  
61 (b)(7)(E)  
62  
63  
64  
65

**SECRET**

66 (a) (U) System Expert: (b)(7)(E)

67 (b) (U) Network Monitoring and Payload Control.

68 (c) (U) (b)(7)(E)

69 (d) (U) Focal Point for Unified Commander:  
70 USSTRATCOM/Command Center, Joint Staff/J38

71 (5) (U) (b)(7)(E)  
72 (b)(7)(E)  
73  
74  
75  
76  
77  
78  
79

80 (a) (U) System Expert: (b)(7)(E)  
81 (b)(7)(E)

82 (b) (U) Network Monitoring and Payload Control: (b)(7)(E)  
83 (b)(7)(E)  
84

85 (c) (U) Focal Point for Commander Requirements: Individual  
86 Unified Commander communications planners or (b)(1) Sec 1.7(e)

87 (d) (U) (b)(7)(E)  
88 (b)(7)(E)

89 (6) (U) Other Government and Commercial Satellite Communications.  
90 (b)(7)(E)  
91  
92

93 2. (U) Mission. Provide command and control connectivity for USSTRATCOM  
94 operations on a global basis in support of peacetime, OPLAN, and contingency  
95 operations.

96 3. (U) Execution. Command and Control (C2) of USSTRATCOM assets, by  
97 their global nature, is highly dependent upon military and civilian satellite  
98 communications systems. USSTRATCOM assists the warfighting Commanders  
99 to ensure effective utilization of these systems by coordinating with the Joint  
100 Staff and the various System Experts.

**SECRET**

101 a. (U) Concept Operations. Command, Control, and Communication  
102 (C3) support (b)(1) Sec 1.7(e) delineated in  
103 the execution paragraph of the base plan.

104 b. (U) Tasks

105 (1) (U) USSTRATCOM. Execute oversight of assigned SATCOM in  
106 support of the POTUS/SECDEF, CJCS, Combatant Commands, and other  
107 agencies.

108 (a) (U) Evaluate health and status of theater SATCOM systems  
109 and develop options for spacecraft movements and/or payload configurations.

110 (b) (U) Recommend spacecraft movements to satisfy warfighting  
111 Combatant Commander's SATCOM requirements.

112  
113 (c) (U) Recommend SATCOM payload reconfiguration when  
114 satellite anomalies occur.

115 (d) (U) Propose SATCOM payload configurations to provide  
116 support to POTUS/SECDEF, CJCS, Combatant Commands, and other federal  
117 agencies.

118 (e) (U) Recommend augmenting C3 requirements with  
119 commercial and Allied SATCOM resources when Military SATCOM is not  
120 sufficient.

121 (f) (U) Provide SATCOM support for theater operations through  
122 (b)(1) Sec 1.7(e)

123 (g) (U) Develop SATCOM analysis based on developed  
124 supporting plans for the Commander and Joint Staff.

125 (h) (U) Develop alternative solutions for identified shortfalls.

126 (i) (U) Reassess and evaluate SATCOM environment and adjust  
127 plans as needed.

128 (2) (U) Supported Commands. Identify space-related C3 and  
129 SATCOM requirements to USSTRATCOM (b)(1) Sec 1.7(e)

130 (b)(1) Sec 1.7(e)

131

132 (3) (U) Component Commands. Be prepared to execute the C3  
133 portions of this plan as modified by CDRUSSTRATCOM.

**SECRET**



**SECRET**

134 c. (U) Special Measures. All task organizations will use standard  
135 Information Security (INFOSEC) procedures and equipment. For joint actions  
136 (other than normal operations) with Unified and Specified Commands, the  
137 Intertheater COMSEC Package (ICP) will be used.

138 4. (U) Administration and Logistics

139 a. (U) Logistics. (N/A)

140 b. (U) Administration. The USSTRATCOM Knowledge Integration Web  
141 (SKIWEB) home page is the primary administration tool and can be accessed  
142 directly via SIPRNET.

143 5. (U) Command and Control

144 a. (U) Command Relationships. (See 8039 Annex J)

145 b. (U) Command, Control, Communications Systems. (See Appendices)

146 Appendices:

147 1 - Information Assurance (Not Used)

148 2 - Satellite Communications (Not Included)

149 3 - Defense Courier Service (Not Used)

150 4 - Foreign Data Exchange (Not Used)

151 5 - Electromagnetic (EM) Spectrum Management (Not Used)

152

153

154

155

156

157

158 Kevin P. Chilton

159 General, USAF

160 Commander

161

162 OFFICIAL

163

164

165

166 (b)(6)

167 CAPTAIN, USN

168 Director, C2 and Communications Systems

**SECRET**

~~SECRET~~

(INTENTIONALLY BLANK)

~~SECRET~~

K-6

~~SECRET~~

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
26 February 2008

- 1 ANNEX N TO USSTRATCOM CONPLAN 8039 (U)  
2 (U) OPR: JFCC SPACE  
3 SPACE OPERATIONS (U)  
4  
5 (U) References:  
6  
7 a. (U) National Space Policy, Oct 06 (S//NF)  
8  
9 b. (U) National Security Space (NSS) Protection Strategy, 30 Nov 04 Ver 5  
10 (S//NF)  
11  
12 c. (U) CJCSI 3121.01A, Standing Rules of Engagement /Standing Rules of  
13 for US Forces, 13 Jun 05 (U) (SROE/SRUF)  
14  
15 d. (U) DOD Directive 3100.10, Space Policy, 9 Jul 99 (U)  
16  
17 e. (U) DOD Directive S-3600.1, Information Operations, 14 Aug 06 (S)  
18  
19 f. (U) Joint Pub 1-02, Department of Defense (DOD) Dictionary of Military &  
20 Associated Terms, 12 Apr 01 (U)  
21  
22 g. (U) DODI 3100.12, Space Support, 14 Sep 00 (U)  
23  
24 h. (U) DODI 3100.14, Space Force Enhancement, 12 Jan 01 (U)  
25  
26 i. (U) DODI 3100.15, Space Control, 19 Jan 01 (U)  
27  
28 j. (U) Joint Pub 3-14, Joint Doctrine for Space Operations, 9 Aug 02 (U)  
29  
30 k. (U) JP 3-13, Joint Doctrine for Information Operations, 13 Feb 06 (U)  
31  
32 l. (U) USSTRATCOM Commander's Strategic Concept, 11 Nov 03 (S/NF)  
33  
34 m. (U) United States Strategic Command (USSTRATCOM) (b)(1) Sec 1.7(e)  
35 (b)(1) Sec 1.7(e) (S/REL)  
36  
37 n. (U) STRATCOM DIRECTIVE (SD) 505-3, Space Support to the Joint Force

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (e), and (g)~~  
~~Declassify on: 26 February 2033~~

~~SECRET~~

# ~~SECRET~~

- 38 Commander/Designated Space Coordinating Authority, Feb 04 (U)  
39  
40 o. (U) SD 515-2, ITWAA Procedures and System Description, 03 Oct 05  
41 (SECRET)  
42  
43 p. (U) SD 523-2, Theater Event System Architecture and Ops,  
44  
45 q. (U) The Commission to Assess United States National Security Space  
46 Management and Organization Final Report, 2001 (U)  
47  
48 r. (U) AFDD 2-2.1, Counterspace Operations, 2 Aug 04 (U)  
49  
50 s. (U) AFDD 2-5, Information Operations, 11 Jan 05 (U)  
51  
52 t. (U) AFTTP 3-1.28, Tactical Employment Space, Mar 05 (S//NF)  
53  
54 u. (U) Space Capstone Threat Assessment, March 2006, NAIC  
55 (SECRET//FGI//NOFORN//MR)  
56  
57 v. (U) Horizontal Command and Control (C2) Integration (HC2I) Concept of  
58 Operations (CONOPS), 20 Dec 05

~~SECRET~~

59 1. (U) Situation

60

61 a. (U) General

62

63 (1) (~~C//REL USA, AUS, GBR~~) US Cyber Operations are a strategic asset  
64 of the United States supporting US National Security Objectives. This annex  
65 provides an overview of relevant space operations and effects supporting  
66 operations executed under CONPLAN 8039. (b)(1) Sec 1.4(a)

67 (b)(1) Sec 1.4(a)  
68  
69  
70  
71  
72

73

74 (2) (~~S//REL USA, AUS, GBR~~) Some cyberspace capabilities operate in  
75 and through the space environment. (b)(1) Sec 1.4(a)

76 (b)(1) Sec 1.4(a)  
77  
78  
79  
80  
81

82

83 b. (U) (b)(1) Sec 1.7(e) Refer to Annex B (Intelligence) (b)(1) Sec 1.7(e)  
84 (b)(1) Sec 1.7(e)

85

86 c. (U) Friendly

87

88 (1) (~~S//REL USA, AUS, GBR~~) The architecture (b)(1) Sec 1.4(a)

89 (b)(1) Sec 1.4(a)

90 may be different in every GCC. Current USSTRATCOM (b)(1) Sec 1.4(a)

91 (b)(1) Sec 1.4(a)  
92  
93

94 capabilities are briefly described below.

95

96 (a) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

97

98 1 (b)(1) Sec 1.4(a)

99

100 2 (b)(1) Sec 1.4(a)

101

102 3 (b)(1) Sec 1.4(a)

103

104 (b) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

SECRET

105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146

1 (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2 (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

3 (b)(1) Sec 1.4(a)

(c) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)

1 (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

2 (b)(1) Sec 1.4(a) Analyses

3 Best accuracy (b)(1) Sec 1.4(a)

(2) (~~S//REL USA, AUS, GBR~~) Additional capabilities. Refer to

(b)(1) Sec 1.4(a)

d. (U) Assumptions. Refer to Base Plan.

2. (U) Mission. Refer to Base Plan and Annex C (Operations).

3. (U) Execution. Refer to (b)(1) Sec 1.7(e)

4. (U) Administration and Logistics

(U) a. (~~S//REL USA, AUS, CAN, GBR~~) Services are responsible to support forces tasked in this Annex. Requirements that cannot be met by a respective service will be coordinated with USSTRATCOM.

b. (U) Reference Base Plan for additional logistics information.

5. (U) Command and Control

a. (U) USSTRATCOM has delegated JFCC SPACE to provide space mission expertise to plan, support, integrate, assess and synchronize efforts for USSTRATCOM, and other combatant commander's operational level requirements for space control operations.

b. (U) CDRUSSTRATCOM has assigned CDR JFCC SPACE as the GSCA to ensure unity of effort by coordinating, developing and conducting operational-level space campaign planning (including contingency and crisis action/adaptive planning and COA development) and strategy development in

# SECRET

147 support of USSTRATCOM and other Combatant Commanders. The GSCA is  
148 the commander designated by CDRUSSTRATCOM to have "Coordinating  
149 Authority" (CA) for the conduct and coordination of global space operations.  
150 CA is a specific consultation relationship between military commanders and  
151 other agencies, not an authority by which command and control may be  
152 exercised. As such, the commander who has been designated as the GSCA can  
153 require consultation between the agencies involved, but cannot compel  
154 agreement. CDRUSSTRATCOM will specify the common tasks to be  
155 coordinated in the establishing directive, without disturbing normal  
156 organizational relationships in other matters.  
157

158 c. (U) The role of the Space Coordinating Authority (SCA) is described and  
159 defined in Joint Publication (JP) 3-0 III.2.d.(2) and Strategic Command  
160 Directive (SD) 505-3, Space Support To Joint Force Commander Or Designated  
161 Space Coordinating Authority. JP 3-0 defines the SCA as being responsible for  
162 coordinating and integrating space capabilities in the operational area, and has  
163 primary responsibility for joint space operations planning, to include  
164 ascertaining space requirements within the joint force. The SCA normally will  
165 be supported by assigned or attached embedded space personnel. The  
166 processes for articulating requirements for space force enhancement products  
167 are established and specifically tailored to the functional area they support,  
168 and result in prioritized requirements. The SCA recommends prioritized space  
169 force enhancement requirements to support the Joint Force Commander's  
170 mission and intent. Utilizing reachback through the JFCC Space at the Joint  
171 Space Operations Center, direct support relationships are established to  
172 provide optimal support to the Joint Force Commander, integrating and  
173 synchronizing space effects within the Joint Force Commander's Joint  
174 Operations Area. To ensure prompt and timely support, the supported GCC  
175 and CDRUSSTRATCOM may authorize direct liaison between the SCA and  
176 applicable component(s) of USSTRATCOM. Joint force Service component  
177 commands should communicate their requirements to the SCA, or designated  
178 representative, to ensure that all space activities are properly integrated and  
179 synchronized.  
180

181 d. (U) C4 Systems. Refer to Base Plan and Annex K (C4 Systems).  
182

183 e. (U) Refer to Base Plan and Annex J (Command Relationships) for  
184 additional Command and Control information.  
185  
186  
187  
188  
189  
190  
191  
192

SECRET

~~SECRET~~

193  
194  
195 Kevin P. Chilton  
196 General, USAF  
197 Commander  
198  
199  
200  
201 OFFICIAL:  
202  
203  
204  
205 WILLIAM L. SHELTON  
206 Lieutenant General, USAF  
207 Commander, JFCC SPACE

~~SECRET~~



**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
28 February 2008

1 ANNEX S TO USSTRATCOM CONPLAN 8039 (U)

2 (U) OPR: JFCC NW J59

3 (b)(1) Sec 1.7(e) (U)

4  
5 (U) References: Refer to the Base Plan.

6  
7 1. (U) Situation. This annex discusses (b)(1) Sec 1.7(e)

8 (b)(1) Sec 1.7(e) capabilities to support CONPLAN 8039.

9  
10 2. (U) Mission. Refer to the Base Plan.

11  
12 3. (U) Execution

13  
14 a. (U) Concept of Operations

15  
16 (1) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
17 provides guidance for (b)(1) Sec 1.4(a) planning and execution in CONPLAN 8039. This  
18 document identifies to planners that USSTRATCOM has chosen to (b)(1) Sec 1.4(a)

19 (b)(1) Sec 1.4(a)

20  
21  
22  
23 includes Appendices and Tabs that addresses how apportioned and non-  
24 apportioned cyberspace (b)(1) Sec 1.4(a)

25 (b)(1) Sec 1.4(a)

26 capabilities and would be included in (b)(1) Sec 1.4(a)

27 (b)(1) Sec 1.4(a)

28 The complete annex is available on the HQ  
USSTRATCOM PDAS Website. (b)(1) Sec 1.4(a) Access is required to review the annex.

29 4. (U) Administration and Logistics. Refer to the Base Plan and Exhibit 4  
30 (Logistics) for each (b)(1) Sec 1.7(e) in the annex.

31 5. (U) Command and Control. Refer to Base Plan, Annex K (Command  
32 Relationships), and Exhibit 5 (Command and Control) for each (b)(1) Sec 1.7(e) in  
33 the annex.

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (c), and (g)~~  
~~Declassify on: 27 February 2033~~

**SECRET**

~~SECRET~~

34

35

36

37

38 Kevin P. Chilton

39 General, USAF

40 Commander

41

42

43

44

45

46 OFFICIAL:

47 Mark H. Owen

48 Brigadier General, USAF

49 Director, Plans and Policy

~~SECRET~~

S-2

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
26 February 2008

1 ANNEX V TO COMMANDER USSTRATCOM CONPLAN 8039 (U)

2 (U) OPR: HQUSSTRATCOM/J53

3 INTERAGENCY COORDINATION (U)

4  
5 References:

6  
7 a. (U) Joint Publication 1-02, Department of Defense Dictionary of  
8 Military and Associated Terms, 12 April 2001 (As Amended Through 20 March  
9 2006)

10  
11 b. (U) Joint Publication 3-0, Joint Operations, 17 Sep 06

12  
13 c. (U) CJCS Manual 6510.1D, Defense in Depth: Information Assurance  
14 (IA) and Computer Network Defense (CND) (U//FOUO), 25 Mar 03. Including  
15 Ch 1, 10 Aug 2004, current as of 18 Mar 2005.

16  
17 d. (U) APPENDIX 12 TO ANNEX C (OPERATIONS) TO JTF-GNO OPORD  
18 05-01 (Global Network Operations) INFORMATION OPERATIONS CONDITION  
19 (INFOCON) EXECUTION PROCEDURES (C/Rel USA, AUS, CAN, GBR, NZL), 22  
20 May 06

21  
22 e. (U) Horizontal Command and Control (C2) Integration (HC2I) Concept  
23 of Operations (CONOPS) (S/Rel USA, AUS, CAN, GBR), 20 Dec 05

24  
25 f. (U) Presidential Decision Directive-62 (PDD-62), Protection Against  
26 Unconventional Threats to the Homeland and Americans Overseas, 22 May 98

27  
28 g. (U) Presidential Decision Directive-63 (PDD-63), Critical Infrastructure  
29 Program, 22 May 99

30  
31 h. (U) National Security Policy Directive 1, "Organization of the National  
32 Security Council System," 13 Feb 2001

33  
34 i. (U) National Security Policy Directive 44, "Management of Interagency  
35 Efforts Concerning Reconstruction and Stabilization," 7 Dec 2005

36  
37 j. (U) 2004 National Response Plan (NRP), Cyber Annex, Dec 04

38  
~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (c), and (g)~~  
~~Declassify on: 26 February 2033~~

**SECRET**

# SECRET

39 k. (U) Homeland Security Presidential Directive 1: Organization and  
40 Operation of the Homeland Security Council. 29 October 2001  
41

42 l. (U) Homeland Security Presidential Directive 7: Critical Infrastructure  
43 Protection. 17 December 2003  
44

45 m. (U) Homeland Security Presidential Directive 8: National  
46 Preparedness. 17 December 2003  
47

48 n. (U) JP 3-08 Vol I & II Interagency, Intergovernmental Organization,  
49 and Nongovernmental Organization Coordination During Joint Operations, 17  
50 March 2006  
51

52 o. (U) National Infrastructure Protection Plan, 22-23 Aug 2006

53 p. (U) Trilateral Memorandum of Agreement among the Department of  
54 Defense, the Justice Department and the Intelligence Community Regarding  
55 Computer Network Attack and Computer Network Exploitation Activities (DOD-  
56 JD-IC MOA) (S//NFS//NF), 9 May 07

57 q. (U) Memorandum of Arrangement between The Department of Defence  
58 of Australia, The Ministry of Defence of The United Kingdom of Great Britain  
59 and Northern Ireland, and The Department Of Defense of The United States of  
60 America on Information Operations Data Exchange, 6 May 03

61 r. (U) 2008 National Response Framework (NRF).

62 s. (U) DODD 3025.1, Military Support to Civil Authorities, January 15,  
63 1993.

64 t. (U) JP 3-28 Civil Support, September 14, 2007.

## 65 1. (U) Situation

### 66 a. (U) General

67 (1) (U) Statement. This Annex provides the basis for interagency  
68 coordination for Cyberspace Operations. It defines the roles and interagency  
69 relationships among United States (U.S.) Strategic Command (USSTRATCOM),  
70 Department of Defense (DOD) organizations, non-DOD U.S. Government  
71 agencies and civilian entities as they pertain to supporting CONPLAN 8039's

72 (b)(1) Sec 1.7(e)

73 (a) (U) (b)(1) Sec 1.7(e)

74 (b)(1) Sec 1.7(e)

75 (b) (U) (b)(1) Sec 1.7(e)

# SECRET

**SECRET**

76 (c) (U) (b)(1) Sec 1.7(e)  
77 (b)(1) Sec 1.7(e)

78 (2) (U) Politico-Military Situation. U.S. reliance on computer systems  
79 and networks is vital to commerce and prosperity and is a critical capability of  
80 the nation's power. Since adversaries can conduct malicious activities that may  
81 jeopardize U.S. interests, including DOD's mission accomplishment and  
82 operations, CDRUSSTRATCOM requires proactive and cooperative interagency  
83 working arrangements with all agencies involved in cyberspace operations. It is  
84 imperative that support be given to the deliberate planning process to ensure  
85 interagency coordination is formalized and communicated to all those involved  
86 in cyberspace operational missions.

87 (3) (U) Policy Coordination

88 (a) (U) National Security Council (NSC)/Policy Coordination  
89 Committees (PCCs). Due to its transnational scope, CONPLAN 8039 can affect  
90 any of the six regional or 11 functional NSC/PCCs. However, the primary  
91 NSC/PCCs affected by CONPLAN 8039 are:

92 1 (U) Defense Strategy, Force Structure, and Planning (chaired  
93 by the Secretary of Defense)

94 2 (U) Counter-Terrorism and National Preparedness (chaired by  
95 the Assistant to the President for National Security Affairs)

96 3 (U) Proliferation, Counter proliferation, and Homeland  
97 Defense (chaired by the Assistant to the President for National Security Affairs)

98 (b) (U) General Guidance. The following highlights general functions  
99 for staff directorate coordination activities:

100 1 (U) Coordination Authority. JP 1-02 defines coordinating  
101 authority as:

102 "A commander or individual assigned responsibility for  
103 coordinating specific functions or activities involving forces of two  
104 or more Military Departments, two or more joint force components,  
105 or two or more forces of the same Service. The commander or  
106 individual has the authority to require consultation between the  
107 agencies involved, but does not have the authority to compel  
108 agreement. In the event that essential agreement cannot be  
109 obtained, the matter shall be referred to the appointing authority.  
110 Coordinating authority is a consultation relationship, not an  
111 authority through which command may be exercised. Coordinating  
112 authority is more applicable to planning and similar activities than  
113 to operations."

114 2 (U) Coordination Relationships. USSTRATCOM will provide  
115 the nature of interagency coordination activities and the service categories.

# SECRET

116 Each agency may participate in operations, operations support and support, as  
117 defined below:

118 a (U) Operations. Actions by agencies to help direct and  
119 coordinate the plan's (b)(1) Sec 1.7(e) (see para 1.a. above). Interagency  
120 coordination for CONPLAN execution is delineated in the Base Plan by (b)(1) Sec 1.7(e)  
121 organization and task. See the Base Plan and (b)(1) Sec 1.7(e)

122 b (U) Operations Support. Actions by agencies to provide  
123 Indications and Warning (I&W), analytical support, tools, and other services.

124 c (U) Support. Actions by agencies to provide policy,  
125 doctrine, guidance, standards, research and development, and other general  
126 support for the cyberspace operations mission.

127 (4) (U) Planning and Execution Coordination. The interconnected and  
128 critical nature of the Defense Information Infrastructure (DII) to the National  
129 Information Infrastructure (NII), the Global Information Infrastructure (GII) and  
130 the GIG fundamentally increases the risk environment for the DOD computers  
131 and computer networks of the GIG. In this environment there is a shared risk,  
132 beyond DOD's control, that extends globally across networks to include the NII,  
133 GII and GIG and geographic boundaries. Cyberspace defense in this complex  
134 environment requires an organization to understand the dynamics of  
135 information processing, to develop and maintain current situation awareness  
136 supported by a Common Operational Picture (COP), and maintain unity of  
137 effort and command. To ensure effective cyberspace operations, Commander,  
138 USSTRATCOM must coordinate regularly with other DOD, non-DOD agencies  
139 and through the Chairman Joint Chiefs of Staff (CJCS) and Joint Staff (JS) to  
140 the POTUS, SECDEF and Cabinet Departments to incorporate, where  
141 applicable, all guidance, perspectives and available information on cyberspace  
142 operations. These include agencies and organizations within DOD, federal  
143 government agencies, state and local government, commercial and civilian  
144 organizations. Interagency coordination will be critical to the support of current  
145 POTUS and SecDef directives such as Presidential Decision Directive (PDD)-62  
146 and PDD-63 and the National Continuity of Operations Plan. Commander,  
147 USSTRATCOM will plan, develop and provide recommendations through the  
148 CJCS and JS (b)(1) Sec 1.7(e)

149 (b)(1) Sec 1.7(e)

152 b. (U) Assumptions. Refer to the Base Plan.

153 c. (U) Legal Considerations. See Base Plan and Appendix 8 (Rules of  
154 Engagement) to Annex C (Operations).

155(U) 2. (~~S//REL USA, AUS, GBR~~) Mission. Refer to the Base Plan.

156 3. (U) Execution

# SECRET

# SECRET

157 a. (U) Concept of Operations. The primary objective of interagency  
158 coordination is effective operational execution of the DOD strategic, global  
159 cyberspace operations mission. Interagency coordination is absolutely vital to  
160 achieving this objective. Commander, USSTRATCOM will use interagency  
161 coordination to:

- 162 o (U) Assist USSTRATCOM cyberspace mission planning and execution  
163 supporting the plan's (b)(1) Sec 1.7(e)
- 164 o (U) Leverage the operational value associated with unity of command.
- 165 o (U) Improve operational situation awareness and information sharing.
- 166 o (~~S//REL USA, AUS, GBR~~) Coordinate, deconflict and integrate mutual  
167 initiatives to include the use of the (b)(1) Sec 1.4(a)  
168 (b)(1) Sec 1.4(a)

169 (1) (U) Commander's Intent. USSTRATCOM Commander's Intent by  
170 (b)(1) Sec 1.7(e) can be found in the Base Plan. Within the Base Plan, interagency  
171 coordination with respect to planning and authorities is a key event:

172 (a) (~~S//REL USA, AUS, GBR~~) Planning. USSTRATCOM may also  
173 require coordination (b)(1) Sec 1.4(a)  
174 USSTRATCOM will also work with the Office of the Secretary of Defense (OSD)  
175 and Joint Staff to (b)(1) Sec 1.4(a)  
176 (b)(1) Sec 1.4(a)

177 (b) (~~S//REL USA, AUS, GBR~~) Authorities. Independent of the scale  
178 of the cyber engagement criteria, the authority will increase as the cyber  
179 engagement criteria grows in sophistication; the cyber engagement criteria may  
180 (b)(1) Sec 1.4(a)  
181

182 (2) (U) (b)(1) Sec 1.7(e) Due to the transregional scope of CONPLAN 8039,  
183 interagency support will be tailored to (b)(1) Sec 1.7(e)  
184 each (b)(1) Sec 1.7(e) Generally, interagency  
185 (b)(1) Sec 1.7(e) is focused on:

186 (a) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Refer to the Base Plan for  
187 (b)(1) Sec 1.4(a)  
188  
189 cyberspace by understanding adversary (b)(1) Sec 1.4(a) During this  
190 (b)(1) Sec 1.4(a) USSTRATCOM, in conjunction with the agency  
191 partners, will:

- 192 1 (U) Continue conducting (b)(1) Sec 1.7(e) NetOps mission.
- 193 2 (~~S//REL USA, AUS, GBR~~) Continue to develop and refine  
194 cyberspace plans (b)(1) Sec 1.4(a) Interagency partners as  
195 appropriate.

# SECRET

**SECRET**

196 3 (~~S//REL USA, AUS, GBR~~) Continue to assist in defining the  
197 DOD requirements from other agency partners, (b)(1) Sec 1.4(a)  
198 (b)(1) Sec 1.4(a)

199 4 (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
200 (b)(1) Sec 1.4(a)  
201

202 5 (~~S//REL USA, AUS, GBR~~) Continue to (b)(1) Sec 1.4(a)  
203 (b)(1) Sec 1.4(a)  
204 (b)(1) Sec 1.4(a) with situational awareness of USSTRATCOM's  
205 (b)(1) Sec 1.4(a) cyberspace mission.

206 (b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) See the Base Plan for  
207 military operations associated with this (b)(1) Sec 1.4(a)  
208 (b)(1) Sec 1.4(a)  
209 (b)(1) Sec 1.4(a) USSTRATCOM, in conjunction  
210 with the agency partners, will:

211 1 (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
212 (b)(1) Sec 1.4(a)

213 2 (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
214 situational awareness to CDRUSSTRATCOM and Staff (b)(1) Sec 1.4(a)  
215 (b)(1) Sec 1.4(a)

216 3 (~~S//REL USA, AUS, GBR~~) Plan (b)(1) Sec 1.4(a)  
217 (b)(1) Sec 1.4(a) and other agency  
218 partners.

219 4 (~~S//REL USA, AUS, GBR~~) Support and facilitate (b)(1) Sec 1.4(a)  
220 (b)(1) Sec 1.4(a) agency partners.

221 (U)5 (~~S//REL USA, AUS, GBR~~) Provide updated interagency  
222 assessment to CDRUSSTRATCOM.

223 6 (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
224 (b)(1) Sec 1.4(a) to Annex A (Task Organization) (b)(1) Sec 1.4(a)  
225 for more information about (b)(1) Sec 1.4(a) operations.

226 (c) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Refer to the Base Plan for  
227 military operations associated with this (b)(1) Sec 1.4(a)  
228 (b)(1) Sec 1.4(a)  
229  
230  
231 (b)(1) Sec 1.4(a) USSTRATCOM, in conjunction with the agency partners,  
232 will:

233 1 (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
234 operations.



**SECRET**

235 2 (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
236 cyberspace situational awareness to CDRUSSTRATCOM and Staff, as well as  
237 agency (b)(1) Sec 1.4(a)

238 3 (~~S//REL USA, AUS, GBR~~) Continue (b)(1) Sec 1.4(a)  
239 (b)(1) Sec 1.4(a) as appropriate, in coordination (b)(1) Sec 1.4(a) other agency partners.

240 4 (~~S//REL USA, AUS, GBR~~) Support and facilitate processing  
241 of (b)(1) Sec 1.4(a) to and from agency partners.

242 (U) 5 (~~S//REL USA, AUS, GBR~~) Provide updated interagency  
243 assessment to the Commander.

244 6 (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) planning and  
245 operations through support to applicable planning and operations groups.

246 (d) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Refer to the Base Plan for  
247 military operations associated with this (b)(1) Sec 1.4(a) The focus of the interagency  
248 effort (b)(1) Sec 1.4(a)  
249 (b)(1) Sec 1.4(a)  
250  
251  
252 (b)(1) Sec 1.4(a) USSTRATCOM,  
253 in conjunction with the agency partners, will:

254 1 (~~S//REL USA, AUS, GBR~~) Continue to (b)(1) Sec 1.4(a)  
255 (b)(1) Sec 1.4(a) as appropriate.

256 2 (~~S//REL USA, AUS, GBR~~) Facilitate the (b)(1) Sec 1.4(a)  
257 (b)(1) Sec 1.4(a) operations through effective interagency coordination.

258 3 (~~S//REL USA, AUS, GBR~~) Support USSTRATCOM  
259 (b)(1) Sec 1.4(a) planning and operations.

260 (U) 4 (~~S//REL USA, AUS, GBR~~) Provide updated assessments to  
261 the Commander and agency partners.

262 5 (~~S//REL USA, AUS, GBR~~) Anticipate (b)(1) Sec 1.4(a)  
263 and (b)(1) Sec 1.4(a) operations.

264 (e) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Refer to the Base Plan for  
265 military operations associated with this (b)(1) Sec 1.4(a) interagency coordination focus  
266 (b)(1) Sec 1.4(a)  
267 (b)(1) Sec 1.4(a) USSTRATCOM in conjunction with the agency partners, will:

268 1 (~~S//REL USA, AUS, GBR~~) Continue (b)(1) Sec 1.4(a)  
269 (b)(1) Sec 1.4(a) as appropriate.

270 (U) 2 (~~S//REL USA, AUS, GBR~~) Facilitate the execution of DOD  
271 support to the primary or coordinating agency(s) through interagency  
272 coordinating as required.

**SECRET**

273 3 (~~S//REL USA, AUS, GBR~~) Provide updated assessments to  
274 the commander and interagency partners regarding (b)(1) Sec 1.4(a)  
275 (b)(1) Sec 1.4(a)

276 (U) 4 (~~S//REL USA, AUS, GBR~~) Provide the Commander with  
277 situational awareness of cyber-related transition requirements from DOD and  
278 agency partners for mutual support.

279 5 (~~S//REL USA, AUS, GBR~~) Anticipate (b)(1) Sec 1.4(a)  
280 (b)(1) Sec 1.4(a) operations.

281 6 (~~S//REL USA, AUS, GBR~~) Provide updated cyber  
282 assessments to the commander and interagency partners regarding conditions  
283 in the (b)(1) Sec 1.4(a)

284 (f) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) Refer to the Base Plan for  
285 military operations associated with this (b)(1) Sec 1.4(a) interagency coordination focus  
286 is on providing support, as applicable and upon request, (b)(1) Sec 1.4(a)  
287 (b)(1) Sec 1.4(a)

288 (b)(1) Sec 1.4(a) USSTRATCOM in conjunction with the agency partners, will:

289 1 (~~S//REL USA, AUS, GBR~~) Continue (b)(1) Sec 1.4(a)  
290 (b)(1) Sec 1.4(a) as appropriate.

291 (U) 2 (~~S//REL USA, AUS, GBR~~) Facilitate the execution of DOD  
292 support to the primary or coordinating agency(s) through interagency  
293 coordinating as required.

294 3 (~~S//REL USA, AUS, GBR~~) Provide the Commander with  
295 situational awareness of cyber-related (b)(1) Sec 1.4(a) DOD and  
296 agency partners for mutual support.

297 4 (~~S//REL USA, AUS, GBR~~) Anticipate (b)(1) Sec 1.4(a) results.

298 5 (~~S//REL USA, AUS, GBR~~) Provide updated cyber  
299 assessments to the commander and interagency partners regarding conditions  
300 in the (b)(1) Sec 1.4(a)

301 b. (U) Tasks and Milestones

302 (1) (U) USSTRATCOM. The following guidance concerning  
303 CDRUSSTRATCOM command responsibilities is provided to assist deliberate  
304 planning and CONPLAN execution.

305 (a) (U) CDRUSSTRATCOM, as the lead Combatant Commander for  
306 cyberspace operations and planning, advocates cyberspace requirements for all  
307 Combatant Commanders, plans and develops national cyberspace operational  
308 requirements, conducts cyberspace operations planning and operations and  
309 supports other combatant commander cyberspace operations efforts.  
310 CDRUSSTRATCOM will focus on planning, policy, processes, mission  
311 coordination, synchronization and integration activities associated with the  
312 cyberspace operations mission. Combatant Commands, Services, Agencies

**SECRET**

313 (C/S/As), components, and supporting forces will focus on operational mission  
314 execution. CDRUSSTRATCOM will interact with C/S/As to include, but not be  
315 limited to, the Joint Staff, SecDef, the Intelligence Community (IC), Law  
316 Enforcement (LE) Agencies, National Infrastructure Protection Center (NIPC)  
317 and the Department of Homeland Security (DHS) to integrate support and  
318 continuously improve the DOD's cyberspace operations processes.

319 (b) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
320 Concept. USSTRATCOM may designate a lead component to establish a (b)(1) Sec 1.4(a)  
321 (b)(1) Sec 1.4(a) to plan, synchronize, collaborate and deconflict  
322 operations for each scenario provided in (b)(1) Sec 1.4(a)

323 (b)(1) Sec 1.4(a)  
324  
325  
326  
327  
328

329 (b)(1) Sec 1.4(a) cyberspace operations in support of the combatant  
330 commander's desired objectives.

331 1 (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) will be offered the  
332 opportunity to assist with (b)(1) Sec 1.4(a)

333 (b)(1) Sec 1.4(a)  
334  
335

336 concurs will be evaluated and adjudicated by CDRUSSTRATCOM. (b)(1) Sec 1.4(a)  
337 members are requested to leverage their agency's or organization's abilities to  
338 support the commander's objectives. (b)(1) Sec 1.4(a)  
339 military control and under SecDef-delegated military authorities.

340 2 (~~S//REL USA, AUS, GBR~~) Close liaison with all (b)(1) Sec 1.4(a)

341 (b)(1) Sec 1.4(a)  
342  
343  
344

345 evolve to meet these requirements.

346 3 (~~S//REL USA, AUS, GBR~~) For (b)(1) Sec 1.4(a) the lead  
347 USSTRATCOM component for the operation will provide the opportunity to  
348 physically and/or virtually participate in all planning activities and provide a  
349 secure and trusted environment that fosters transparency of operational  
350 equities. The (b)(1) Sec 1.4(a) will serve the following purposes:

351 a. (~~S//REL USA, AUS, GBR~~) Assist in the (b)(1) Sec 1.4(a)  
352 (b)(1) Sec 1.4(a)

353 b. (~~S//REL USA, AUS, GBR~~) Provide information in support  
354 of a (b)(1) Sec 1.4(a) to Combatant  
355 Commanders, customers, planners and operators.

**SECRET**

**SECRET**

356 c (~~S//REL USA, AUS, GBR~~) Participate in and make  
357 recommendations for the (b)(1) Sec 1.4(a)  
358 (b)(1) Sec 1.4(a)

359 (U) d (~~S//REL USA, AUS, GBR~~) Assist in coordination,  
360 collaboration, synchronization, and deconfliction or courses of action in  
361 response to combatant commander's requirements, for both deliberate and  
362 crisis action planning.

363 (U) e (~~S//REL USA, AUS, GBR~~) Consider, advise and  
364 recommend solutions on all risks posed by planned or on-going operations.

365 (U) f (~~S//REL USA, AUS, GBR~~) Act as a representative authority  
366 or liaison (as determined by each member's organization or agency) on issues  
367 related to or surfacing from planned or on-going operations.

368 (U) g (~~S//REL USA, AUS, GBR~~) Assist in the formal  
369 coordination between the lead USSTRATCOM component and interagency  
370 senior officials which must [also] be in coordination with the Joint Staff.

371 h (~~S//REL USA, AUS, GBR~~) An adjunct membership to the  
372 (b)(1) Sec 1.4(a)  
373 (b)(1) Sec 1.4(a) cyberspace  
374 operations, in some cases with differing restrictions or legal requirements. The  
375 (b)(1) Sec 1.4(a)  
376  
377 cyberspace environment.

378 i (~~S//REL USA, AUS, GBR~~) The (b)(1) Sec 1.4(a) at  
379 least (b)(1) Sec 1.4(a) (and other participants, as invited) to  
380 assess and address (b)(1) Sec 1.4(a)  
381 (b)(1) Sec 1.4(a)  
382  
383 authority level, or make recommendations for (b)(1) Sec 1.4(a) lead  
384 does not have approval authority.

385 (c) (U) HQ USSTRATCOM/J2 and Components will coordinate with  
386 the IC and its appropriate organizations to identify, manage, monitor, and  
387 advocate for cyberspace intelligence requirements, standardized reporting,  
388 (b)(1) Sec 1.7(e) and general intelligence support. In  
389 addition, specified component(s) will also (b)(1) Sec 1.7(e)  
390 (b)(1) Sec 1.7(e) planning activities to focus monitoring, collection and  
391 analysis activities. The primary goal is to provide (b)(1) Sec 1.7(e) and value-  
392 added analysis for the CDRUSSTRATCOM to conduct global cyberspace  
393 missions.

394 (d) (U) USSTRATCOM will organize, advocate and coordinate  
395 cyberspace operational exercises across C/S/As. USSTRATCOM will advocate  
396 for standardized training and education requirements and coordinate  
397 cyberspace operational modeling and simulation efforts with applicable

**SECRET**

# SECRET

398 agencies. USSTRATCOM will conduct deliberate and crisis action planning and  
399 produce a Joint Monthly Readiness Review (JMRR) for the DOD cyberspace  
400 operational mission and force structure. This will be based in large measure  
401 on inputs from the JFCC NW, the JTF GNO, JIOWC, and also on frequent  
402 interaction with C/S/As.

403 (e) (U) USSTRATCOM will develop, coordinate and advocate for  
404 cyberspace operations deliberate planning, concepts, policy, doctrine,  
405 (b)(1) Sec 1.7(e) and mission-level requirements. In addition,  
406 USSTRATCOM will assist in development and support of command and DOD  
407 partnerships with selected industry, academia and allies, including  
408 development of the necessary Memoranda of Agreement/Understanding. This  
409 will include establishing policies and resolving policy issues.

410 (f) (U) USSTRATCOM will support development of partnerships and  
411 relationships with DOD and non-DOD agencies, private industry and coalition  
412 partners. In addition, USSTRATCOM will help develop and advocate for  
413 common education, training and awareness standards for users, operators,  
414 and administrators. Finally, they will help ensure cyberspace operational  
415 requirements are reflected in plans, requirements and Courses of Action  
416 (COAs).

417 (g) (U) The USSTRATCOM/J006, will provide the required legal  
418 interpretations, liaison, related services, and inputs to support this plan. J006  
419 will interpret appropriate legal policies and procedures in the development of  
420 partnerships and relationships with DOD and non-DOD agencies, private  
421 industry and coalition partners and allies. J006 will also work closely with the  
422 LE/CI centers in developing potential COAs, which fall under appropriate  
423 LE/CI authorities and coordinate with LE/CI legal staffs.

424 (2) (U) Coordination with Combatant Commanders

425 (a) (U) JTF GNO.

426 1 (U) JTF GNO has directive authority with DOD agencies,  
427 other than IC agencies, to counter strategic, global network attacks and  
428 intrusions and, has coordinating authority for responding to attacks and  
429 intrusions directed at DOD intelligence networks. The coordinating authority,  
430 with respect to DOD Intelligence networks, shall be exercised consistent with  
431 the Defense Criminal Investigative Service's responsibility for the network  
432 security for intelligence systems.

433 2 (U) JTF GNO receives agency incident reports and  
434 responses in compliance with (b)(1) Sec 1.7(e)  
435 (b)(1) Sec 1.7(e) and national directives as appropriate. JTF  
436 GNO also coordinates with the DOD (b)(1) Sec 1.7(e)  
437 (b)(1) Sec 1.7(e)  
438 (b)(1) Sec 1.7(e) to maintain status of DOD IC  
439 networks and significant incidents or threats to those networks. The IC will

# SECRET

**SECRET**

440 exercise management and security oversight of the DOD IC networks while  
441 maintaining routine coordination with and reporting to JTF GNO.

442 3 (U) JTF GNO also supports and coordinates with the  
443 National Response Coordination Group (NCRCG) on behalf of USSTRATCOM.  
444 Per ref j, the NCRCG is an interagency forum where organizations responsible  
445 for a range of activities (technical response and recovery, law enforcement,  
446 intelligence, and defensive measures) coordinate for the purposes of preparing  
447 for and executing an efficient and effective response to a cyber incident.

448 4 (U) (b)(1) Sec 1.7(e) JTF GNO  
449 (b)(1) Sec 1.7(e) cyberspace  
450 operations. (b)(1) Sec 1.7(e) administrative, logistics, resource  
451 management, public affairs, and personnel support. JTF GNO maintains an  
452 (b)(1) Sec 1.7(e)  
453  
454  
455  
456 may provide operational and technical analytical resources to augment JTF  
457 GNO.

458 5 (U) (b)(1) Sec 1.7(e)  
459 (b)(1) Sec 1.7(e) receives operational direction from JTF GNO.

460 6 (U) Law Enforcement/Counter-Intelligence (LE/CI). JTF  
461 GNO has a full-time LE/CI Center for coordinating LE/CI activities in support  
462 of cyberspace operations. DOD LE/CI agencies have assigned full and/or part  
463 time LE/CI agents to support the JTF GNO mission from each of the LE/CI  
464 agencies, including Naval Criminal Investigative Service, Defense Criminal  
465 Investigative Service, Air Force Office of Special Investigations (AFOSI), Army  
466 Criminal Investigations Command, and Army Intelligence and Security  
467 Command. A SJA provides necessary legal advice to the Commander JFCC  
468 NW, Commander JTF GNO and their staffs. The SJA works closely with the  
469 LE/CI Center in developing potential COAs which fall under appropriate LE/CI  
470 authorities and coordinates with LE/CI legal staffs.

471 (U) (b) (~~S//REL USA, AUS, GBR~~) JFCC NW. See Annex J, Command  
472 Relationships.

473 c. (U) Coordinating Instructions. This CONPLAN cannot task the  
474 Interagency partners. The following are recommendations for the conduct of  
475 the CONPLAN 8039 mission.

476 (1) (U) USSTRATCOM Coordination Activities. Within mission and  
477 resource constraints, USSTRATCOM will coordinate with appropriate national  
478 agencies, C/S/As and other agencies for cyberspace operations planning and  
479 execution. USSTRATCOM will coordinate with the following organizations:

**SECRET**

480 (a) (U) (b)(1) Sec 1.7(e)  
481 (b)(1) Sec 1.7(e)  
482

483 (b) (U) Intelligence Community (IC). Provide USSTRATCOM with  
484 intelligence standards, policy and guidance for intelligence support for  
485 cyberspace operations and foreign disclosure.

486 (c) (U) National Infrastructure Protection Center (NIPC). Provide  
487 USSTRATCOM with NII and LEA alerts and warnings, federal agency and  
488 private sector coordination and deconfliction, forensic analysis, LE/CI advice  
489 and support, NII situational awareness, COP, reporting for cyberspace  
490 operations, standardized processes and procedures, GIG  
491 coordination/deconfliction, intelligence warning, I&W, and planning and  
492 execution support.

493 (d) (U) Office of the Assistant Secretary of Defense, Networks and  
494 Information Integration (OASD/NII). OASD/NII, will provide USSTRATCOM  
495 with DOD policy, oversight and guidance, and support C3I, Computers,  
496 Intelligence, Surveillance and Reconnaissance (C4ISR) resource priorities for  
497 cyberspace operations. In addition, OASD/NII will provide Information  
498 Assurance (IA) training and certification standards, Information Technology  
499 architecture standards, acquisition support, and research and technology.  
500 CDRUSSTRATCOM will coordinate with OASD/NII to advocate C/S/A  
501 cyberspace operations requirements and priorities, coordination, feedback and  
502 policies.

503 (e) (U) Joint Staff (JS). Provide USSTRATCOM with rules of  
504 engagement (ROE), cyberspace operational requirements validation, joint policy  
505 and doctrine, joint exercise support, and plans and policy support.  
506 USSTRATCOM will coordinate with the JS for cyberspace operational  
507 execution, combatant commander cyberspace operational requirements and  
508 resource priorities, C4ISR, training, readiness, plans and policy, coordination  
509 and situational awareness (SA).

510 (f) (U) Supporting Combatant Commanders. Provide USSTRATCOM  
511 with operational impact assessments, cyberspace operational plans, operations  
512 and Information Security (INFOSEC) implementation, cyberspace operations  
513 resource requirements and priorities, cyberspace operations reporting,  
514 Information Operations Condition (INFOCON) implementation and component  
515 cyberspace operations readiness. USSTRATCOM will coordinate with all  
516 Combatant Commanders for planning, operations and resource requirements,  
517 cyberspace operational integration, coordination and deconfliction, cyberspace  
518 operations intelligence warning, I&W, attack assessment, and situational  
519 awareness.

520 (g) (U) Services. Provide USSTRATCOM with operations impact and  
521 technical assessments, plans, operations and INFOCON implementation,  
522 resource priorities and requirements, cyberspace operations readiness and

**SECRET**

**SECRET**

523 reporting and LE/CI intelligence support. USSTRATCOM will coordinate with  
524 the Services for intelligence and vulnerability information, red teaming,  
525 cyberspace operational integration, intelligence I&W, and attack assessments.  
526 The Services will advocate their requirements and priorities, contribute to  
527 overall situational awareness, conduct cyberspace operations coordination and  
528 ensure systems and operations, integration and deconfliction.

529 (h) (U) (b)(1) Sec 1.7(e) Provide USSTRATCOM

(b)(1) Sec 1.7(e)

537 (i) (U) (b)(1) Sec 1.7(e) Provide CDRUSSTRATCOM (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

545 (b)(1) Sec 1.7(e) for requirements and priorities, standards, policy and procedures,  
546 operational direction, and situational awareness.

547 (j) (U) (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

555 (k) (U) Law Enforcement/Counter-Intelligence (LE/CI). DOD LE/CI  
556 agencies will provide USSTRATCOM with full and/or part time LE/CI agents  
557 from each of the LE/CI agencies, including NCIS, DCIS, AFOSI, USACID and  
558 INSCOM.

559 (l) (U) (b)(1) Sec 1.7(e) Provide USSTRATCOM (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)



# SECRET

564 (m) (U) Department of State (DOS). Coordinate and provide  
565 guidance for COAs requiring diplomatic action or have diplomatic  
566 ramifications.

567 (n) (U) Department of Commerce (DOC). Coordinate and provide  
568 guidance for COAs requiring economic action or have economic ramifications.

569 (o) (U) Department of Justice (DOJ). Per ref n, in exceptional  
570 circumstances and with appropriate authorization, military forces may also  
571 conduct missions to help the Department of Justice or other Federal law  
572 enforcement agencies (LEAs) assist federal, state, or local LEAs. Accordingly  
573 USSTRATCOM could be called upon to coordinate and provide guidance for  
574 cyber-related COAs requiring legal action or have legal ramifications.

575 (p) (U) Department of Homeland Security (DHS)

576 1 (U) Coordinate with USSTRATCOM and provide guidance for  
577 COAs related to homeland security and the protection of the United States.

578 2 (U) Per ref j Department of Homeland Security/Infrastructure  
579 Analysis and Infrastructure Protection/National Cyber Security Division  
580 (DHS/IAIP/NCSD) will act as the focal point for the security of non-DOD U.S.  
581 interests in cyberspace for purposes of analysis, warning, information sharing,  
582 vulnerability reduction, mitigation, and aiding national recovery efforts for  
583 critical infrastructure information systems.

584 3 (U) In conjunction with the DOS, DHS will coordinate with  
585 USSTRATCOM and the interagency community to work with foreign countries  
586 and international organizations to strengthen the protection of U.S. critical  
587 information infrastructures and those foreign critical information  
588 infrastructures on which the United States relies and may impact DOD  
589 networks.

590 (q) (U) USNORTHCOM. USSTRATCOM will coordinate with  
591 USNORTHCOM for domestic cyber related incidents which will likely result in  
592 requests for assistance (RFAs) from other federal, state, tribal and local  
593 agencies, if their capabilities are exceeded. The Primary Agency in need of  
594 cyberspace support submits a Request for Assistance (RFA) to the Office of the  
595 Secretary of Defense (OSD) Executive Secretary for planning and assessment, if  
596 established the Defense Coordinating Officer (DCO) will validate the  
597 requirements on the RFA, the RFA will be forwarded to the Joint Director of  
598 Military Support (JDOMS) and the Assistant Secretary of Defense for Homeland  
599 Defense (ASD[HD]), a copy is provided to USNORTHCOM J3, JDOMS produces  
600 an EXORD for approval and the Secretary of Defense (SECDEF) in coordination  
601 with ASD(HD) approves it, and JDOMS issues the SECDEF-approved EXORD .  
602 When directed, USJFCOM, in coordination with USSTRATCOM, provides  
603 conventional forces to the Commander, US Northern Command, for Defense  
604 Support of Civil Authorities in support of other Federal, state, tribal and local  
605 government agencies for cyber related domestic incidents.

# SECRET

# SECRET

606 (2) (U) Additional USSTRATCOM Coordination Activities

607 (a) (U) Joint Activities. Joint Activities can provide a wealth of  
608 information, enabling tools, data and analysis to enhance USSTRATCOM's  
609 ability to identify critical nodes, networks, and other points of influence  
610 regarding adversaries and U.S. vulnerabilities that can affect U.S. interests in  
611 cyberspace. Some of the Joint Activities that USSTRATCOM can leverage when  
612 planning for cyberspace operations are the Joint Warfighting Center, Joint  
613 Warfare Analysis Center, Joint C4ISR Battle Center, Joint Program Office for  
614 Special Technical Countermeasures (JPO-STC), National Defense University  
615 (NDU) and Service War Colleges, Defense Advanced Research Projects Agency  
616 (DARPA), and Space and Naval Warfare Systems Command (SPAWAR).

617 (b) (U) Federal Government. As stated in ref n, The Homeland  
618 Security Act of 2002 established the DHS whose mission is to lead the unified  
619 national effort to secure America by preventing and deterring terrorist attacks  
620 and protecting against and responding to threats and hazards to the nation.  
621 As such, DHS is the lead federal agency for homeland security. While the most  
622 visible support occurs during domestic emergencies or major disasters, the  
623 majority of DOD's efforts are directed toward civilian law enforcement or  
624 intelligence agencies. This assistance is known as civil support within the  
625 defense community because the assistance will always be in support of a lead  
626 federal agency. Requests for assistance from another agency may be  
627 predicated on mutual agreements between agencies or stem from a Presidential  
628 designation of a Federal Disaster Area or a Federal State of Emergency. DOD  
629 typically only responds after the resources of other federal agencies, state and  
630 local governments to include National Guard and NGOs have been exhausted  
631 or when military assets are required. The DOD works closely with other  
632 Federal agencies in various domestic arenas. In addition to participating in  
633 interagency steering groups and councils, DOD is a partner in several national  
634 level incident management and emergency response plans such as the Federal  
635 Response Plan (as modified by the Initial National Response Plan, Cyber  
636 Annex). It is possible that USSTRATCOM could be called upon to assist in the  
637 event of a cyber-related disaster or domestic emergency. Accordingly  
638 USSTRATCOM will coordinate possible supporting efforts and plan with the  
639 Critical Infrastructure Assurance Office, National Security Telecommunications  
640 and Information Systems Security Committee, Office of the Manager of the  
641 National Communications System, National Institute of Standards and  
642 Technology and Department of Energy National Laboratories. Outside of JTF  
643 GNO's responsibility to coordinate with the NCRCG as stated above, all  
644 domestic cyber-related incidents which will likely result in RFAs from other  
645 federal agencies will be coordinated through USNORTHCOM.

646  
647 (c) (U) Intelligence Community. Intelligence support provides the  
648 JFC with a timely, complete, and accurate understanding of the environment  
649 and potential adversaries. The method for collecting intelligence in support of  
650 cyberspace operations is generally the same as that for any other military

SECRET

# SECRET

651 operation and is conducted in accordance with JP 2-01, Joint and National  
652 Intelligence Support to Military Operations. Managing the cyber intelligence  
653 collection, analysis, production, and dissemination for a CONPLAN 8039 crisis  
654 action may be complicated by non-USG civilians, especially members of IGOs  
655 and NGOs, who may be sensitive to the perception that they are being used to  
656 gather intelligence. This sensitivity may be based on the viewpoint that  
657 intelligence gathering is a provocative act and damages an individual's claim to  
658 impartiality. However, general information provided by personnel from IGOs  
659 and NGOs may corroborate intelligence gained from other sources. Generally,  
660 the best approach to information sharing with the NGOs and international  
661 civilian community is to keep the focus on complete transparency in sharing  
662 operational information and developing a shared situational awareness and  
663 understanding of the objectives to achieve the mission. However, classified  
664 information will only be shared with or released to individuals with the  
665 appropriate security clearance and need to know. In addition to IGOs and  
666 NGOs, USSTRATCOM will coordinate with the National Intelligence Council  
667 and the national intelligence agencies to support intelligence needs set forth in  
668 this plan.

669  
670 (d) (U) Coalition Partners. Unity of effort is essential to coordinate  
671 cyberspace operations in joint and multinational environments, requiring  
672 coordination not only between Services and US agencies, but also among all  
673 coalition partners. USSTRATCOM must consider cyber-related priorities  
674 between DOD requirements and those of other USG agencies, the country  
675 team, coalition or UN forces, NGOs, and any international cyber-related  
676 organizations, that may be established. Close communications should be  
677 established with all elements to ensure that their cyberspace requirements are  
678 fully understood by the USSTRATCOM lead component to enable effective  
679 planning and effective cyberspace operations. USSTRATCOM will coordinate  
680 with the North Atlantic Treaty Organization (NATO) and other bilateral and  
681 multilateral coalitions as required.

682 (e) (U) Commonwealth Nations. The Commonwealth of Nations,  
683 usually known as "the Commonwealth" is a voluntary association of 53  
684 independent sovereign states, all of which are former possessions of the British  
685 Empire, except for Mozambique and the United Kingdom itself. The  
686 Commonwealth is an international organization through which countries with  
687 diverse social, political, and economic backgrounds cooperate within a  
688 framework of common values and goals. These include the promotion of  
689 democracy, human rights, good governance, the rule of law, individual liberty,  
690 egalitarianism, free trade, multilateralism, and world peace. Currently  
691 USSTRATCOM has two cyber-related agreements with Commonwealth nations:

692 1 (C//REL USA, AUS, GBR) Tri-lateral Memorandum of  
693 Agreement (MOA) on IO data exchange. (b)(1) Sec 1.4(a)

694 (b)(1) Sec 1.4(a)

# SECRET

**SECRET**

695 (b)(1) Sec 1.4(a) and the Department of Defense of the United States of  
696 America, are signatories of a tri-lateral MOA on IO data exchange. The  
697 objective of this MOA (b)(1) Sec 1.4(a)

698 (b)(1) Sec 1.4(a)  
699  
700  
701  
702  
703

704 2 (U) International Computer Network Defense Coordination  
705 Working Group. The International Computer Network Defense Coordination  
706 Working Group (ICCWG) is composed of five participating militaries: Australia,  
707 Canada, New Zealand, United Kingdom and United States. The ICCWG was  
708 established to exchange and conduct multilateral information  
709 assurance/computer network defense (IA/CND) up to the Top Secret level for  
710 the goal of strengthening information networks; to improve the confidentiality,  
711 integrity and availability of information systems; and improve the prediction,  
712 detection and response capabilities. USSTRATCOM/J51 is designated as the  
713 United States National Lead; JTF GNO is responsible for the operational  
714 mission.

715 (f) (U) Educational Activities. Far reaching changes are  
716 concurrently taking place in every major area of human life, perhaps most  
717 notably in how we conduct cyberspace warfare. Further, we expect information  
718 technology to continue its spectacular climb, greatly impacting cyberspace  
719 operations. Therefore, it is imperative that USSTRATCOM engage with  
720 educational activities and industry to understand and acquire new cyberspace  
721 operational capabilities that may affect DOD cyberspace. Some educational  
722 activities USSTRATCOM engages with are: (b)(1) Sec 1.7(e)

723 (b)(1) Sec 1.7(e)

724 (b)(1) Sec 1.7(e) and Security and  
725 Service postgraduate schools.

726 (3) (U) Industry Relationships. For many of the same reasons  
727 outlined above, USSTRATCOM engages with educational activities, it will also  
728 coordinate with industry through the National Security Telecommunications  
729 Advisory Committee (NSTAC), PDD-63 Critical Infrastructure Sector  
730 Coordinators and Industry Information Sharing and Analysis Centers.  
731 USSTRATCOM may selectively establish relationships with industry that  
732 leverage councils and committees with both government and industry  
733 members. These top-level relationships will provide USSTRATCOM with a  
734 forum for gaining and sharing insights on common and developing  
735 telecommunications and security issues, major developments and advanced  
736 technologies. Industry participants on NSTAC will gain an understanding of  
737 DOD requirements and priorities, as well as insights into possible synergies  
738 between the DOD and industry for cyberspace operations.

**SECRET**

**SECRET**

739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776

(4) (U) Government-Industry Forums. The USSTRATCOM staff participates in the established (b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e)

operations. Concurrently, National Science Foundation participants gain an understanding of USSTRATCOM technology needs and priorities for cyberspace operations and information assurance.

(5) (U) US Army. See Annex J (Command Relationships)

(6) (U) Navy Forces (NAVFOR). See Annex J (Command Relationships)

(7) (U) Marine Forces (MARFOR) See Annex J (Command Relationships)

(8) (U) Commander, Air Force Forces (COMAFFOR). See Annex J (Command Relationships)

(9) (U) GNOSC. The GNOSC consists of the Operations Center and DOD CERT and is co-located with JTF GNO. The GNOSC provides both the network operations view to JTF GNO and is the technical "arm" of JTF GNO via the DOD CERT.

(10) (U) JWRAC. The JWRAC is assigned administratively to DISA, and is under TACON of JTF GNO. Comprised of Reserve Component personnel, the JWRAC has the mission to "conduct analysis of content and data resident on publicly accessible DOD web sites across the full range of military operations."

Kevin P. Chilton  
General, USAF  
Commander

Official:

Mark H. Owen  
Brigadier General, USAF  
Director of Plans and Policy

~~SECRET~~

(INTENTIONALLY BLANK)

~~SECRET~~

V-20

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
26 February 2008

1  
2 (U) ANNEX Y TO CDRUSSTRATCOM CONPLAN 8039 (U)

3 (U) OPR: JIOWC/JSSC  
4 STRATEGIC COMMUNICATION (U)

5  
6 (U) References: Refer to the Base Plan.

7  
8 a. (U) National Security Strategy of the United States of America,  
9 March 2006 (U)

10 b. (U) National Defense Strategy of the United States of America,  
11 March 2005 (U)

12 c. (U) National Military Strategy of the United States of America, 2004 (U)

13 d. (U) US National Strategy for Public Diplomacy and Strategic  
14 Communication, 2007 (U)

15 e. (U) Presidential Decision Directive (PDD) 68, 30 April 1999, International  
16 Public Information (U)

17 f. (U) 2005 Contingency Planning Guidance (U)

18 g. (U) Strategic Planning Guidance, 22 March 2006 (U)

19 h. (S) (b)(1) Sec 1.4(a)  
20 (b)(1) Sec 1.4(a) (S)

21 i. (S) // Rel USA, GBR, AUS (b)(1) Sec 1.4(a)  
22 (b)(1) Sec 1.4(a) (S)

23 j. (U) Quadrennial Defense Review (QDR) Execution Roadmap for Strategic  
24 Communication, 25 Sep 2006 (U)

25 k. (U) National Strategy to Public Diplomacy and Strategic Communications

26 1. (U) Situation

27 a. (U) General

28 (1) (U) The United States faces a growing threat from hostile state, and  
29 non-state actors with the intent and capability to threaten US vital interests.

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (c), and (g)~~  
~~Declassify on: 26 February 2033~~

**SECRET**

# SECRET

30 Effective SC by the whole of government is critical to deterring attacks by  
31 hostile actors. America must effectively use words, actions, and images to  
32 demonstrate the country's will and means to impose costs, while encouraging  
33 restraint. According to the 2006 QDR Execution Roadmap, the term strategic  
34 communication (SC) is defined as, "Focused U.S. government processes and  
35 efforts to understand and engage key audiences in order to create, strengthen  
36 or preserve conditions favorable to advancing national interests and policies  
37 through the use of coordinated information, themes, plans, programs, and  
38 actions with other elements of national power." The POTUS directs the  
39 nation's overall SC effort. Based on Presidential guidance, DOS leads  
40 America's public diplomacy efforts with foreign state and non-state actors.  
41 DOD provides extensive lethal and non-lethal capabilities that should  
42 supplement efforts, by DOS and other USG agencies, to engage key audiences  
43 to advance US interests and policies. USSTRATCOM planners must consider  
44 that words, actions, and images, from the highest to lowest ranking members  
45 of the Armed Forces, can profoundly impact the success or failure of USG  
46 policies and interests. The CDRUSSTRATCOM must be in continuous contact  
47 with the leaders in Washington and other Combatant Commanders as  
48 required, to ensure USSTRATCOM efforts are in concert with the overall USG  
49 SC effort, pursuant to Presidential guidance.

50 (2) (U) USG Guidance. USG guidance is fluid in nature, responsive to  
51 the global geo-political situation, internal US politics, mood of the American  
52 populace, and opinions of key US and world leaders. USG policies and  
53 objectives are delineated through speeches, statements, and documents by the  
54 POTUS, Secretary of State, Congress, and other influential leaders.  
55 USSTRATCOM SC efforts should support the new U.S National Strategy for  
56 Public Diplomacy (PD) and Strategic Communication, dated June 2007, which  
57 provides three strategic objectives for engaging foreign audiences: (1) America  
58 must offer a positive vision of hope and opportunity that is rooted in our most  
59 basic values; (2) With our partners, we seek to isolate and marginalize violent  
60 extremists who threaten the freedom and peace sought by civilized people of  
61 every nation, culture and faith; (3) America must work to nurture common  
62 interests and values between Americans and peoples of different countries,  
63 culture and faiths across the world. The 2006 NSS establishes eight national  
64 security objectives: (1) To champion human dignity; (2) To strengthen alliances  
65 against terrorism; (3) To defuse regional conflicts; (4) To prevent threats from  
66 weapons of mass destruction; (5) To encourage global economic development  
67 (6) To expand the circle of development; (7) To cooperate with the other centers  
68 of global power; and (8) To transform America's national security institutions to  
69 meet the challenges and opportunities of the Twenty- First Century. Additional  
70 clarification on national objectives as they pertain to specific hostile state and  
71 non-state actors are available via multiple open source channels.

72  
73 (3) (~~S//REL USA, AUS, GBR~~) Country/Regional Perspective. Military  
74 planners must consider the perceptions, attitudes, and beliefs of each actor, or

SECRET



**SECRET**

75 target audience. Although communications may be conducted in space or  
76 cyberspace, the target audiences reside within Geographic Combatant  
77 Command (GCC) areas of responsibility. Every country and region across the  
78 globe is unique, with varying opinions and attitudes. (b)(1) Sec 1.4(a)

79 (b)(1) Sec 1.4(a)  
80  
81  
82  
83  
84  
85  
86  
87

88 (b)(1) Sec 1.4(a) and the respective Geographic Combatant Command's  
89 Public Affairs Office, SC Working Group, and Joint Interagency Coordination  
90 Group.

91  
92 b. (U) Adversary. See Annex B (Intelligence) (b)(1) Sec 1.7(e)

93 (b)(1) Sec 1.7(e)  
94

95 c. (U) Friendly

96  
97 (1) (U) See Base Plan for the general friendly situation.  
98

99 (2) (U) DOS. The DOS-led SC and PD Policy Coordinating Committee  
100 (PCC) supports USG policy and interests as directed by the POTUS. In June  
101 2007, this interagency committee published the US National Strategy for Public  
102 Diplomacy and Strategic Communication, under the guidance of Amb. Karen  
103 Hughes. This strategy, which supplements the NSS and NMS, provides  
104 overarching USG guidance for US diplomatic and communication efforts. A  
105 DOD link to the State Department is the DOD Strategic Communication  
106 Integration Group (SCIG) Secretariat, which serves as a conduit for the  
107 Combatant Commands to surface SC issues for interagency consideration, via  
108 an Executive Committee, to the Deputy Secretary of Defense. Other conduits  
109 to the State Department include joint inter-agency task forces, joint inter-  
110 agency coordination groups, political advisors, and for USSTRATCOM, J5 and  
111 JIOWC LNOs at the Pentagon, plus conferences, meetings, seminars, and other  
112 means as appropriate.  
113

114 (4) (U) Geographic Combatant Commands (GCCs). The GCCs use  
115 varying processes and organizational structures to plan, execute, and assess  
116 SC efforts. Based on Department of State (DOS) and Office of the Secretary of  
117 Defense/Public Affairs (OSD/PA) guidance, the GCCs develop themes,  
118 messages, and talking points for target audiences in their AORs.  
119 USSTRATCOM planners should leverage existing processes and organizations,

**SECRET**

SECRET

120 such as the GCC SC Working Groups and Strategic Effects Cells/Divisions, as  
121 well as the JIOWC's GCC Support Teams to ensure unity of effort.  
122

123 (5) (U) See base plan and Annex A (Task Organization) for 8039's  
124 friendly force capabilities, which are drawn from USSTRATCOM global mission  
125 areas for full-spectrum capabilities (b)(1) Sec 1.7(e)  
126

127 (6) (U) See applicable OPLAN and force deployment lists for the  
128 Combatant Commands that will be involved in the operation.  
129

130 (7) (U) Assumptions. Refer to the Base Plan.  
131

132 2. (U) Mission. Refer to the Base Plan  
133

134 3. (U) Execution

135 a. (U) Concept of Operations

136 (1) (S//REL USA, AUS, GBR) The purpose of CONPLAN 8039 is to  
137 ensure that the U.S. military can operate in cyberspace (b)(1) Sec 1.4(a)  
138 (b)(1) Sec 1.4(a)

139 providing our own forces the freedom of action in cyberspace. The USG  
140 (b)(1) Sec 1.4(a)

141  
142  
143  
144 (b)(1) Sec 1.4(a) . OSD/PA provides public affairs guidance  
145 to the GCC Public Affairs Offices (PAOs), reinforcing USG (b)(1) Sec 1.4(a)  
146 (b)(1) Sec 1.4(a)

147  
148  
149 in coordination with DOS efforts. This annex provides a framework to facilitate  
150 the integration and synchronization of DOD SC capabilities as part of an  
151 overarching USG cohesive effort to accomplish the mission, focusing on:  
152 (b)(1) Sec 1.4(a)

153 (b)(1) Sec 1.4(a) SC efforts should support US  
154 strategic objectives and considerations (b)(1) Sec 1.4(a) as identified in  
155 the base plan.

156 (2) (U) Overall Plan Objectives and End State. Refer to the Base Plan.  
157

158 (3) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) SC actions (b)(1) Sec 1.4(a)  
159 (b)(1) Sec 1.4(a) operations. Day-to-day operations should emphasize (b)(1) Sec 1.4(b)  
160 (b)(1) Sec 1.4(a)

161

**SECRET**

162 (b)(1) Sec 1.4(a) SC planners  
163 are tasked to develop a communications strategy that will (b)(1) Sec 1.4(a)

164 (b)(1) Sec 1.4(a)  
165

166 power to be effective. The planning, execution, and assessment of SC actions

167 (b)(1) Sec 1.4(a) should be closely

168 coordinated with the applicable GCCs, (b)(1) Sec 1.4(a)

169 (b)(1) Sec 1.4(a)  
170

171

172 (4) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a) SC planners should  
173 revise SC actions based on assessed success or failure to achieve desired

174 (b)(1) Sec 1.4(a)  
175  
176  
177  
178  
179

180 (5) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

181 (b)(1) Sec 1.4(a)  
182  
183  
184  
185  
186  
187  
188  
189  
190

191

192 (6) (U) (b)(1) Sec 1.7(e) SC efforts will continue to (b)(1) Sec 1.7(e)

193 (b)(1) Sec 1.7(e)  
194  
195  
196  
197  
198

199 conduct of operations in Cyberspace.” SC actions should focus on (b)(1) Sec 1.7(e)

200 (b)(1) Sec 1.7(e)  
201

202

203 (7) (S//REL USA, AUS, GBR) (b)(1) Sec 1.4(a)

204 The overall SC effort during (b)(1) Sec 1.4(a)

205 (b)(1) Sec 1.4(a)  
206  
207

**SECRET**

SECRET

208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252

(b)(1) Sec 1.4(a)

(8) (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a) SC  
(b)(1) Sec 1.4(a)

USSTRATCOM will (b)(1) Sec 1.4(a) In addition,  
USSTRATCOM will provide support to the effected GCC, as required, for  
(b)(1) Sec 1.4(a)

(a) (U) Desired SC Effects which help or support (b)(1) Sec 1.7(e)  
(b)(1) Sec 1.7(e)

1. (U) Minimize adversary cyberspace activities to conduct  
aggressive actions against US interest. cyberspace activities by adversaries  
(b)(1) Sec 1.7(e)

supported by the following actions:

2. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) cyberspace.

3. (~~S//REL USA, AUS, GBR~~) Conduct cyberspace (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a)

4. (~~S//REL USA, AUS, GBR~~) (b)(1) Sec 1.4(a)  
(b)(1) Sec 1.4(a) cyberspace.

(U) 5. (~~S//REL USA, AUS, GBR~~) Protect and defend friendly  
information systems and content.

SECRET

253  
254  
255  
256

6. (~~S//REL USA, AUS and GBR~~) (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a) cyberspace capabilities.

257  
258  
259  
260  
261  
262  
263  
264  
265

(9) (~~S//REL USA, AUS, CAN, GBR~~) USSTRATCOM Role. (b)(1) Sec 1.4(a)

(b)(1) Sec 1.4(a)

266  
267  
268

have been tailored for audiences in their AORs. USSTRATCOM SC planners should also leverage the habitual, working relationships between the JIOWC and the GCCs to ensure unity of effort.

269  
270  
271

(10) (~~S//REL USA, AUS, GBR~~) End State. The common end-state for all

(b)(1) Sec 1.4(a)

272

(11) (U) Specific Guidance

273  
274  
275  
276

(a) (U) The SC goal is for DOD to plan, integrate, synchronize, disseminate and

(b)(1) Sec 1.7(e)

277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287

(b) (U) CDRJIOWC is CDRUSSTRATCOM's SC lead and as such must be kept informed of all USSTRATCOM

(b)(1) Sec 1.7(e) In times of crisis, the JIOWC Operations Center (OPCENTER) will maintain continuous contact with the USSTRATCOM Headquarters (HQ) GOC, USSTRATCOM senior leadership, POLAD, and PAO. The entire JIOWC will be matrixed as required to support SC planning, execution, assessment and decision making. The JIOWC

(b)(1) Sec 1.7(e)

(b)(1) Sec 1.7(e) USSTRATCOM staff and other personnel working SC issues as required.

288  
289  
290  
291

(c) (U) GCC SC staffs should leverage USSTRATCOM-wide capabilities, such as the USSTRATCOM J2, J3, and J5, PAO, JFCC NW, and JIOWC. The JIOWC's GCC Support Teams and JSSC provide additional sources of SC planning experience across multiple GCC AORs.

**SECRET**

292 (d) (~~S//REL USA, AUS, GBR~~) JFCC/SCC/JTF planners should  
293 surface key SC related issues, especially those involving interagency  
294 coordination primarily through the GCCs Joint Interagency Coordination  
295 Groups (JIACGs), POLADs, and Strategic Communications Working Groups  
296 (SCWGs). The CDR JIOWC serves as the USTRATCOM link to the DOD SCIG  
297 Secretariat. The Secretariat holds weekly SC Video-Telecommunication  
298 Conferences (VTCs), attended by the Combatant Commands, Joint Public  
299 Affairs Support Element (JPASE), (b)(1) Sec 1.4(a) and  
300 other organizations involved in the DOD SC planning process. This VTC  
301 provides a forum for planners to surface key SC issues that may impact  
302 deterrence operations, execution, or planning.

303 (e) (U) SC plans must be tailored for diverse target audiences, such  
304 as: (b)(1) Sec 1.7(e)  
305 (b)(1) Sec 1.7(e)  
306  
307  
308  
309  
310

311 (12) (U) (b)(1) Sec 1.7(e) SC planners need to  
312 determine if the disseminated USG communications (b)(1) Sec 1.7(e)  
313 (b)(1) Sec 1.7(e)  
314  
315  
316 (b)(1) Sec 1.7(e) USSTRATCOM related actions, such as key  
317 speeches by the command leadership. The JIOWC, via the USSTRATCOM J2,  
318 can also (b)(1) Sec 1.7(e)  
319 (b)(1) Sec 1.7(e)

320 (13) (U) (b)(1) Sec 1.7(e) the impact of USG  
321 communication efforts requires baseline data by (b)(1) Sec 1.7(e)  
322 (b)(1) Sec 1.7(e)  
323  
324  
325  
326 (b)(1) Sec 1.7(e) USSTRATCOM  
327 maintains a limited (b)(1) Sec 1.7(e)  
328 (b)(1) Sec 1.7(e)

329 b. (U) Tasks

330 (1) (U) USSTRATCOM Public Affairs Office. See Annex F (Public Affairs).  
331 PAO will provide PA guidance for the command and conduct (b)(1) Sec 1.7(e) for  
332 statements or speeches made by USSTRATCOM leadership. The PAO

**SECRET**

333 coordinates the development of PA guidance, to include talking points, with  
334 OSD/PA and other Combatant Commands as required.

335 (2) (U) JIOWC. JIOWC will coordinate SC planning efforts with the  
336 GCCs. JIOWC provides SC planning support to USSTRATCOM components  
337 and GCCs as required. During crisis situations, JIOWC will maintain  
338 continuous contact with the USTRATCOM GOC, SCIG, and GCC staffs as  
339 required.

340 (3) (U) JFCCs and JTF GNO will maintain continuous contact with the  
341 USTRATCOM GOC during crisis situations. USSTRATCOM Component  
342 Commands should coordinate SC related efforts with the JIOWC, leveraging the  
343 JIOWC's GCC Support Team's relationships with the GCC SC and IO staffs.

344 (4) (U) Other. See Base Plan for tasks within (b)(1) Sec 1.7(e) as  
345 appropriate.

346 c. (U) Coordinating Instructions

347 (1) (U) This document is effective for planning upon receipt and  
348 execution upon approval of the overall base plan as well as the (b)(1) Sec 1.7(e)  
349 (b)(1) Sec 1.7(e)

350 (2) (~~S//REL USA, AUS, GBR~~) USSTRATCOM Component Commands  
351 will integrate planning efforts to (b)(1) Sec 1.4(a) with  
352 the applicable GCCs. Commands should leverage JIOWC GCC Support Teams  
353 to conduct (b)(1) Sec 1.4(a)  
354 (b)(1) Sec 1.4(a)

355 (3) (~~S//REL USA, AUS, GBR~~) CDRUSSTRATCOM will coordinate with  
356 Combatant Commanders in order to develop and provide those commanders  
357 (b)(1) Sec 1.4(a) See CDRUSSTRATCOM  
358 support plans for specific details.

359 d. (U) Definitions

360 (1) (U) Public Diplomacy (PD): Those overt international public  
361 information activities of the USG designed to promote US foreign policy  
362 (b)(1) Sec 1.7(e)  
363  
364 institutions and their counterparts abroad (JP 3-53 and JP 1-02). The DOS has  
365 the lead within the USG for PD.

366 (2) (U) (b)(1) Sec 1.7(e) DOD activities  
367 (b)(1) Sec 1.7(e)  
368  
369

# SECRET

370 communication. (b)(1) Sec 1.7(e)  
371 environment in support of USG information activities through efforts that may  
372 include, (b)(1) Sec 1.7(e)

373 (b)(1) Sec 1.7(e)

374  
375  
376  
377  
378

379 (3) (U) Military Diplomacy (MD): The ability to support those activities  
380 and measures U.S. military leaders take to engage military, defense and  
381 government officials of another country to communicate USG policies and  
382 messages and to build defense and coalition relationships. (Derived from  
383 March, 2004 National Military Strategic Plan for the War on Terrorism)

384 (4) (U) Public Affairs (PA): Those public information, command  
385 information, and community relations' activities directed toward both the  
386 external and internal publics with interest in the DOD. (JP 3-61).  
387 USTRATCOM PAO is lead for the command, and will coordinate with OSD/PA  
388 and the applicable GCC PAO.

389 (5) (U) Military Information Operations (IO): The integrated employment  
390 of the core capabilities of (b)(1) Sec 1.7(e)

391 (b)(1) Sec 1.7(e)

392 in  
393 concert with specified supporting capabilities (information assurance, physical  
394 security, counter-intelligence, physical attack, and combat communications)  
395 and related capabilities (public affairs, civil military operations, and defense  
396 support to public diplomacy) (b)(1) Sec 1.7(e)

397 (b)(1) Sec 1.7(e)

398 (JP 3-13,  
399 Feb 07) USSTRATCOM components should leverage the existing working  
400 relationships between the JIOWC GCC Support Teams and the GCC IO staffs,  
to integrate and synchronize SC with IO efforts, to achieve the Combatant  
Commander's desired effects on local, regional, and global audiences.

401 4. (U) Administrative and Logistics. See Base Plan.

402 a. (U) SC personnel and administrative support will be furnished by  
403 supporting commands in accordance with Service directives, Command  
404 Arrangements Agreements (CAA), Memorandums of Understanding (MOU),  
405 Task Force CONOPS, and the logistics concept for support operations outlined  
406 in CDRUSSTRATCOM plans and directives.

407 b. JIOWC will coordinate with USSTRATCOM Strategic Effects Cells and  
408 other DOD SCWGs to help synchronize SC across the interagency

# SECRET



~~SECRET~~

409 5. (U) Command and Control. CDRJIOWC is CDRUSSTRATCOM's SC lead,  
410 and as such must be kept informed of all USSTRATCOM (b)(1) Sec 1.7(e)  
411 (b)(1) Sec 1.7(e) In times of crisis, the JIOWC  
412 JOC will maintain continuous contact with the USTRATCOM HQ GOC,  
413 USSTRACOM senior leadership, POLAD, and PAO. The JIOWC will be matrixed  
414 as required to support SC planning, execution, assessment and decision  
415 making. The JIOWC GCC Support Teams will maintain continuous contact  
416 with the applicable GCC SC planning staffs. The JIOWC's Joint SC Support  
417 Cell will maintain close contact with the SCIG at the Pentagon, USSTRATCOM  
418 staff and other personnel working SC issues as required. See paragraph 5.  
419 "Command and Control" of Base Plan; Annex J (Command Relationships), and  
420 Annex K (Command, Control, Communications, and Computers (C4) Systems)  
421 to Base Plan as appropriate.

422  
423  
424  
425

426 Kevin P. Chilton  
427 General, USAF  
428 Commander

~~SECRET~~

~~SECRET~~

(INTENTIONALLY BLANK)

~~SECRET~~

Y-12

**SECRET**

HEADQUARTERS, US STRATEGIC COMMAND  
OFFUTT AIR FORCE BASE, NE 68113-6500  
28 February 2008

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43

ANNEX Z TO USSTRATCOM CONPLAN 8039 (U)  
(U) OPR: HQUSSTRATCOM/J53  
DISTRIBUTION (U)

1. (U) ~~Distribution of this document will be on a strict "need to know" basis with limited distribution.~~
2. (U) ~~Consistent with a need to know, supporting commands may reproduce and distribute this plan to assigned forces as required to fulfill mission requirements, and as required for the preparation of supporting plans. In addition, the plan is available electronically on the USSTRATCOM SIPRNET/GCCS Homepage.~~

~~Classified by: Multiple Sources~~  
~~Reason: 1.4(a), (e), and (g)~~  
~~Declassify on: 26 February 2033~~

# SECRET

44  
45  
46  
47

## (U) Table of Distribution (U)

<u>DISTRIBUTION</u>	<u>OFFICE CODE</u>	<u>NO. COPIES</u>
Joint Staff/J7 CWPD	J7	12
OSD		
CHIEF OF STAFF, US		
ARMY		
CHIEF OF NAVAL		
OPERATIONS		
CHIEF OF STAFF, USAF		
CMDT, MARINE CORPS		
CMDT, COAST GUARD		
DISA		
DLA		
NGA		
NSA		
DIA		
DTRA		
USCENTCOM	J3	1
	J5	1
USEUCOM	ECJ3	1
	ECJ5	1
USNORTHCOM	J3	1
	J5	1
USPACOM	J3	1
	J5	1
USSOCOM	SOJ3	1
	SOJ5	1
USSOUTHCOM	SCJ3	1
	SCJ5	1
USJFCOM	J2	1
	J3	
	J5	
USTRANSCOM	J5	1
USELEMNORAD (US ONLY)	N/J3	1
	N/J5	1
HQ ACC	A3	1
	A3	1

# SECRET

~~SECRET~~

<u>DISTRIBUTION</u>	<u>OFFICE CODE</u>	<u>NO. COPIES</u>
HQ AMC	A3	1
	A4	1
	XO	1
	TACC	1
HQ AFSPC	XO	1
	A8	1
	14AF	1
	SWC	1
NNSOC	N3	1
NETWARCOM	N3	1
	N9	1
COMMARFORSTRAT		1
HQ SMDC	G5	1
8 AF	A2/INR	1
	TFC 204	1
	8 IWF	1
20 AF	DOME	1
	TFC 214	
HQ USAFE	A8	1
HQ PACAF	A8	1
JWAC	J31	1
HQ AIA	A3	1
	AFWIC	1
	67IW	1
	NASIC	1
DEFENSE SUPPLY CENTER	DSCP- OMP/CC	1
20th IS/TMF	CCOZ	1
Cheyenne Mountain Operations Center	J5	1
480 IG		1
DET 1 608 AOG	SMD	1
Office Naval Intelligence (ONI)		1
COMNAVMETOCCOM		1
AFGW Agency		1
HQ Air Force Reserve Command	AFRC/A3	1
National Guard Bureau	A3	1
Commander, HQ AFOSI	A3	1
Director, NCIS	0022B	1

~~SECRET~~

**SECRET**

<b><u>DISTRIBUTION</u></b>	<b><u>OFFICE CODE</u></b>	<b><u>NO. COPIES</u></b>
USSTRATCOM (Internal Distribution)	J1	1
	J2	1
	J3	2
	J4	1
	J5	3
	J6	1
	J7	1
	J8	1
	GISC	1
	Joint Functional Component Command Global Strike and Integration (JFCC GSI)	J3 J5
Joint Functional Component Command Integrated Missile Defense (JFCC IMD)	J5 J3	1 1
Joint Functional Component Command Intelligence, Surveillance, Reconnaissance (JFCC ISR)	OPS PLANS	1 1
Joint Functional Component Command Network Warfare (JFCC NW)	J3 J5	1 1
Joint Functional Component Command-Space (JFCC SPACE)		1
Joint Information Operations Warfare Command (JIOWC)		1
STRATCOM Center for Combating Weapons of Mass Destruction (SCC WMD)		1
Joint Task Force Global Network Operations (JTF GNO)	J3 J5	1 1
NSA Rep to USSTRATCOM		1
CIA Rep to USSTRATCOM		1
DIA Rep to USSTRATCOM		1
NGA Rep to USSTRATCOM		1
NRO Rep to USSTRATCOM		1
NASA Rep to USSTRATCOM		1
DISA Rep to USSTRATCOM		1
USSTRATCOM NAOC	Plans	2

48

49

50

**SECRET**

Z-4

**SECRET**

51 Kevin P. Chilton  
52 General, USAF  
53 Commander

54

55

56

57

58

59 OFFICIAL:

60

61

62

63

64 Mark H. Owen  
65 Brigadier General, USAF  
66 Director, Plans and Policy

**SECRET**

Z-5

~~SECRET~~

(INTENTIONALLY BLANK)

~~SECRET~~

Z-6



**NATIONAL  
SECURITY  
ARCHIVE**

This document is from the holdings of:

The National Security Archive

Suite 701, Gelman Library, The George Washington University

2130 H Street, NW, Washington, D.C., 20037

Phone: 202/994-7000, Fax: 202/994-7005, [nsarchiv@gwu.edu](mailto:nsarchiv@gwu.edu)