APPENDIX D

IPSP EMERGENCY ACTION PLAN (EAP)

NATURAL DISASTERS. Natural disasters include fires, floods, hurricanes, and any phenomena that would result in the inadvertent loss, compromise, or destruction of classified material. When such a situation occurs, the senior Marine or Civilian Employee present will execute the EAP.

1. Fire after duty hours: Should a fire occur around or within Building 1, or any Secondary Control Point (SCP), the Command Security Manager/CMCC Custodian/SCP Custodian will:

a. Notify the Fire Department and Military Police by dialing "911" and report the location and extent of the fire.

b. If the fire occurs during duty hours, secure all classified material in a GSA approved container, vault, or secure room designated as Open Storage Secret (OSS).

c. If the fire occurs after duty hours, ensure the CMCC Vault door, GSA approved container, or SCP is secured before leaving the area.

d. If safe, use all local means to extinguish or control the fire until the fire department arrives. Fire extinguishers are located throughout the building and basement.

e. If after duty hours, and as soon as possible, notify the Command Security Manager, Assistant Security Manager, CMCC Custodian, and/or SCP Custodian.

f. Under no circumstances will anyone subject themselves or their subordinates to possible death or injury to protect classified material from fire.

g. When the Fire Department/Military Police arrive, they will immediately be informed of and admitted to the secure areas. Efforts will be made to get names and identification numbers of all emergency personnel going into secure areas or being exposed to classified material only after the emergency is over.

h. The Security Manager/Assistant, CMCC Custodian, or SCP Custodian will, to the maximum extent possible, ensure that only emergency personnel are allowed into secure areas. When given the "ALL CLEAR" signal from emergency personnel, the vault will be locked or two guards must be placed in the secure area until the Command Security Manager/CMCC Custodian conduct a post-emergency inventory.

i. If the intensity of the fire is such that the area must be abandoned, maintain a surveillance of the general area to prevent unauthorized persons from entering, to the best of your ability.

2. Hurricanes, Floods, and other Natural Phenomena. The danger presented by these conditions are not likely to be as sudden as that presented by fire. The primary objective in case of hurricane, flood, etc., is to secure and waterproof classified material and computers to protect them from wind, water, or destruction until the emergency has passed.

a. Prior to Hurricanes (DWC-1C), the Command Security Manager, Security Assistant, CMCC Custodian, and/or SCP Custodian will waterproof all classified material and gear in GSA approved containers or approved OSS areas. All classified computers will be unplugged and waterproofed with plastic as necessary. All other logs, documents, and other important papers, etc., will also be safeguarded accordingly.

b. If there is damage to the CMCC Vault, SCP, or OSS designated area from a hurricane, flood, or other phenomena, the Command Duty Officer (CDO), or other person on the scene, will immediately contact the Command Security Manager, Assistant Security Manager, CMCC Custodian, and/or SCP Custodian and inform them of the extent of damage.

c. Two persons will be posted, if necessary, as a guard force to prevent unauthorized access to classified material until CMCC personnel arrive.

d. The CMCC will coordinate the removal of classified material, if required, to a location pre-determined by the Command Security Manager, that has the ability to safeguard the classified material at the respective level.

e. All SCPs will coordinate the removal of classified material, if required, to the CMCC (primary), or a location pre-determined by the Command Security Manager, that has the ability to safeguard the classified material at the respective level.

3. Loss of Power resulting from a Natural Disaster

a. Per SECNAV M-5510.36, Restricted Areas designated as OSS are required to safeguard SECRET material by one of the following methods:

(1) In the same manner prescribed for Top Secret;

(2) In a GSA approved security container, modular vault, or vault without supplemental controls;

(3) In a non-GSA-approved container having a built-in combination lock. One of the following supplemental controls are required:

(a) The location housing the security container is subject to continuous protection by cleared guard or duty personnel;

(b) A cleared guard or duty personnel shall inspect the area once every four hours;

(c) An IDS with the personnel responding to the alarm within 15 minutes of the alarm annunciation.

b. In the event of IDS failure as a result of power loss, the Security Manager, Assistant Security Manager, CMCC Custodian, and/or SCP Custodian will coordinate one of the protection measures to ensure the continuous protection of classified material.

HOSTILE ACTIONS. Hostile Actions include, bomb threats, riots, or civil uprisings. In all cases, the assumption will be made that classified material is a target. All actions must be directed to prevent unauthorized personnel from gaining access to classified material by securing, or evacuating the material as conditions dictate. There are three threat stages of hostile action emergencies. These stages will be carried out by CMCC personnel only.

1. Stage One - (Potential Threat)

a. Threat source - Operations in high risk environment.

b. Time frame - Several days to several months.

c. Action - Precautionary Emergency Protection as outlined under Terrorist Actions below.

2. Stage Two - (Probable Threat)

a. Threat source - Probability of hostile attack.

b. Time frame - From one to several days.

c. Action - Possible Emergency Evacuation as outlined under Emergency Evacuations below.

3. Stage Three - (Imminent Threat)

a. Threat source - Attack by hostile forces.

b. Time frame - Imminent.

c. Action - Immediate Emergency Protection or Evacuation as outlined under Terrorist Actions and Emergency Evacuations below.

4. Bomb Threat. In the event of a bomb threat, the Provost Marshal's Office (PMO) will be notified by dialing "9-1-1". Classified material will be secured in the CMCC vault or SCP. The vault will be locked and all classified material accounting records will be removed from the building. Personnel will wait outside the building at a safe distance

until the arrival of the military police and EOD Team. The building will not be re-entered until the "ALL CLEAR" signal is given by EOD personnel.

TERRORIST ACTIONS. Acts of terrorism range from threats of terrorism, assassinations, kidnappings, hijackings, bomb scares and bombings, cyber-attacks (computer-based), to the use of chemical, biological, and nuclear weapons. All actions must be directed to prevent unauthorized personnel from gaining access to classified material by securing, or evacuating the material as conditions dictate. There are five threat stages of terrorist action. These stages will be carried out by CMCC personnel only.

1. Low Condition - Green; low risk of terrorist attacks. The following Protective Measures may be applied:

a. Refining and exercising preplanned Protective Measures;

b. Ensuring personnel receive training on departmental, or agency specific Protective Measures; and

c. Regularly assessing facilities for vulnerabilities and taking measures to reduce them.

2. Guarded Condition - Blue; general risk of terrorist attack. In addition to the previously outlined Protective Measures, the following may be applied:

a. Checking communications with designated emergency response or command locations;

b. Reviewing and updating emergency response procedures; and

c. Providing the public with necessary information.

3. Elevated Condition - Yellow; significant risk of terrorist attacks. In addition to the previously outlined Protective Measures, the following may be applied:

a. Increasing surveillance of critical locations;

b. Coordinating emergency plans with nearby jurisdictions;

c. Assessing further refinement of Protective Measures within the context of current threat information; and

d. Implementing, as appropriate, contingency and emergency response plans.

4. High Condition - Orange; high risk of terrorist attacks. In addition to the previously outlined Protective Measures, the following may be applied:

a. Coordinating necessary security efforts with armed forces or law enforcement personnel;

b. Taking additional precaution at public events;

c. Preparing to work at an alternate site or with a dispersed workforce;

d. Restricting access to essential personnel only.

5. Severe Condition - RED; severe risk of terrorist attacks. In addition to the previously outlined Protective Measures, the following may be applied:

a. Assigning emergency response personnel and pre-positioning specially trained teams;

b. Monitoring, redirecting or constraining transportation systems;

c. Closing public and government facilities; and

d. Increasing or redirecting personnel to address critical emergency needs.

EMERGENCY EVACUATION. Emergency evacuation is that action taken to move classified material to a safe place to prevent unauthorized access caused by fire, hurricane, flood, other natural phenomena, hostile action, or terrorist action.

1. Emergency evacuation will only be executed when directed by the Base Commander or Command Security Manager. The Primary Classified Storage area will be the CMCC Vault located in Building 1. During non-working hours and when directed, the Command Duty Officer (CDO) will:

a. Attempt to contact CMCC personnel and the Command Security Manager using the Emergency Recall Roster (located in the CDO Binder) or the CMCC Access Roster (located on the outside of the CMCC door). If CMCC personnel cannot be contacted, the CDO will obtain the combination cards (SF-700) for the CMCC and Vault door from the Emergency Operations Center (EOC), Rm E100, located at Building 1, and will carry out the Evacuation Plan accordingly until they can be reached.

b. The Command Security Manager or Security Assistant must appoint at least two persons to evacuate the classified material, and contact Military Police to provide armed escort for the evacuation.

c. Ensure a Government Vehicle with driver is readily available for pick-up and delivery of classified material during evacuation.

d. Post a Military Policeman armed guard at the vault entrance and vehicle until all classified material is loaded onto the Government Vehicle.

e. After all classified material has been gathered and packed, the armed guards will escort and protect the total evacuation of all classified material to include unloading and safeguarding it at the new location.

EMERGENCY PROTECTION. Emergency protection actions include collecting all classified materials not needed for immediate operational use, and securing them in the CMCC Vault or a GSA approved container.

1. Emergency protection procedures will only be executed when directed by the Base Commander, Command Security Manager, or other competent authority.

a. All classified material will be locked up in a GSA approved container, vault, or OSS.

b. All other publications, logs, and correspondence will be packed and prepared for evacuation.

2. Any other protection actions deemed necessary by the Security Manager will also be completed during this time.

EMERGENCY DESTRUCTION. Emergency destruction of classified material may be required due to fire, natural disaster, civil disturbance, terrorist activities, or enemy action. These action may lead to the loss or compromise of classified information, to which emergency destruction is required to minimize the risk of unauthorized disclosure through the recovery of classified information, if necessary, following such events.

1. Emergency destruction will only be executed by the CO, Command Security Manager, Assistant Security Manager, CMCC Custodian, SCP Custodian, classified material originator, and/or personnel identified by the CO or Command Security Manager.

2. Paper-based classified material shall be destroyed utilizing one of the following methods:

a. Crosscut shredding

b. Burning

c. Wet pulping

d. Chemical decomposition

e. Pulverizing/disintegrating

3. Classified IT equipment and electronic medial shall be destroyed utilizing one of the following methods:

a. Overwriting;

b. Degaussing;

c. Sanding, or

d. Physical destruction (mutilation).

4. The priority for the destruction of classified material shall be organized by the level of protection against unauthorized disclosure in the interest of national security.

a. The unauthorized disclosure of TOP SECRET material could reasonably be expected to cause exceptionally grave damage to national security and should be destroyed first.

b. The unauthorized disclosure of SECRET material could reasonably be expected to cause serious damage to national security and should be destroyed after all TOP SECRET material has been destroyed. If the command does not possess any TOP SECRET material, SECRET material should be destroyed first.

c. The unauthorized disclosure of CONFIDENTIAL material could reasonably be expected to cause damage to national security and should be destroyed after all TOP SECRET and SECRET material has been destroyed. If the command does not possess any TOP SECRET or SECRET material, CONFIDENTIAL material should be destroyed first.

d. Controlled Unclassified Information (CUI) may be destroyed by any means approved for the destruction of classified information. Destroy paper CUI using cross cut shredders that produce particles that are 1mm by 5mm. Destruction of CUI in the form of electronic media can be performed by clearing, purging, or physical destruction.

e. Foreign Government Information (FGI) shall be destroyed in the same manner as U.S. classified information of the equivalent level, except where otherwise required by international treaty or agreement.

5. Contact the National Security Agency/Central Security Service (NSA/CSS) System and Network Analysis Center at (410)854-6348 or via e-mail at SNAC@radium.ncsc.mil, to obtain technical guidance concerning appropriate methods, equipment, and standards for destroying classified electronic media, IT equipment, electronic components, and other similar or associate materials.

SAMPLE DOCUMENT INVENTORY SHEET

Subject	Document Date	Classification	Document Control Number	Disposition	Name/Signature of person taking action
Widgets required for MEU Deployment	18 May 09	SECRET	54008-9236-A-01	Destroyed 9249	Butler, S.
OPORD 3-08	4 Mar 08	SECRET	34708-8064-B-03	Transferred to HQMC	Lejeune, J.
Hard Drive		SECRET		54008-7245-A-06	

Maintaining one spreadsheet per security container allows subsequent document numbers to simply continue with the next number. Documents in different containers are differentiated by separate container numbers. Commands with the same RUC but many different staff agencies with multiple SCPs can simply use a separate command identifier. For example, HQMC can use the commonly known Department, Division, and Branch identifiers. A document controlled by Security Division of Plans, Policies and Operations, controlled on 24 August 2009, in container A, document number 01 would appear like, PS-9236-A-01.

TABLE-1
JULIAN DATE CALENDAR
(PERPETUAL-NON LEAP YEARS)

DAY	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	DAY
1	001	032	060	091	121	152	182	213	244	274	305	335	1
2	002	033	061	092	122	153	183	214	245	275	306	336	2
3	003	034	062	093	123	154	184	215	246	276	307	337	3
4	004	035	063	094	124	155	185	216	247	277	308	338	4
5	005	036	064	095	125	156	186	217	248	278	309	339	5
6	006	037	065	096	126	157	187	218	249	279	310	340	6
7	007	038	066	097	127	158	188	219	250	280	311	341	7
8	008	039	067	098	128	159	189	220	251	281	312	342	8
9	009	040	068	099	129	160	190	221	252	282	313	343	9
10	010	041	069	100	130	161	191	222	253	283	314	344	10
11	011	042	070	101	131	162	192	223	254	284	315	345	11
12	012	043	071	102	132	163	193	224	255	285	316	346	12
13	013	044	072	103	133	164	194	225	256	286	317	347	13
14	014	045	073	104	134	165	195	226	257	287	318	348	14
15	015	046	074	105	135	166	196	227	258	288	319	349	15
16	016	047	075	106	136	167	197	228	259	289	320	350	16
17	017	048	076	107	137	168	198	229	260	290	321	351	17
18	018	049	077	108	138	169	199	230	261	291	322	352	18
19	019	050	078	109	139	170	200	231	262	292	323	353	19
20	020	051	079	110	140	171	201	232	263	293	324	354	20
21	021	052	080	111	141	172	202	233	264	294	325	355	21
22	022	053	081	112	142	173	203	234	265	295	326	356	22
23	023	054	082	113	143	174	204	235	266	296	327	357	23
24	024	055	083	114	144	175	205	236	267	297	328	358	24
25	025	056	084	115	145	176	206	237	268	298	329	359	25
26	026	057	085	116	146	177	207	238	269	299	330	360	26
27	027	058	086	117	147	178	208	239	270	300	331	361	27
28	028	059	087	118	148	179	209	240	271	301	332	362	28
29	029		088	119	149	180	210	241	272	302	333	363	29
30	030		089	120	150	181	211	242	273	303	334	364	30
31	031		090		151		212	243		304		365	31

TABLE-2
JULIAN DATE CALENDAR
(FOR LEAP YEARS ONLY)

DAY	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	DAY
1	001	032	061	092	122	153	183	214	245	275	306	336	1
2	002	033	062	093	123	154	184	215	246	276	307	337	2
3	003	034	063	094	124	155	185	216	247	277	308	338	3
4	004	035	064	095	125	156	186	217	248	278	309	339	4
5	005	036	065	096	126	157	187	218	249	279	310	340	5
6	006	037	066	097	127	158	188	219	250	280	311	341	6
7	007	038	067	098	128	159	189	220	251	281	312	342	7
8	008	039	068	099	129	160	190	221	252	282	313	343	8
9	009	040	069	100	130	161	191	222	253	283	314	344	9
10	010	041	070	101	131	162	192	223	254	284	315	345	10
11	011	042	071	102	132	163	193	224	255	285	316	346	11
12	012	043	072	103	133	164	194	225	256	286	317	347	12
13	013	044	073	104	134	165	195	226	257	287	318	348	13
14	014	045	074	105	135	166	196	227	258	288	319	349	14
15	015	046	075	106	136	167	197	228	259	289	320	350	15
16	016	047	076	107	137	168	198	229	260	290	321	351	16
17	017	048	077	108	138	169	199	230	261	291	322	352	17
18	018	049	078	109	139	170	200	231	262	292	323	353	18
19	019	050	079	110	140	171	201	232	263	293	324	354	19
20	020	051	080	111	141	172	202	233	264	294	325	355	20
21	021	052	081	112	142	173	203	234	265	295	326	356	21
22	022	053	082	113	143	174	204	235	266	296	327	357	22
23	023	054	083	114	144	175	205	236	267	297	328	358	23
24	024	055	084	115	145	176	206	237	268	298	329	359	24
25	025	056	085	116	146	177	207	238	269	299	330	360	25
26	026	057	086	117	147	178	208	239	270	300	331	361	26
27	027	058	087	118	148	179	209	240	271	301	332	362	27
28	028	059	088	119	149	180	210	241	272	302	333	363	28
29	029	060	089	120	150	181	211	242	273	303	334	364	29
30	030		090	121	151	182	212	243	274	304	335	365	30
31	031		091		152		213	244		305		366	31

(USE IN 2004, 2008, 2012, 2016, ETC)