

Sign-In Sheet for HSERC Members Or their Voting Representatives

August 15, 2002

Environmental Coordinator
UH Environmental Center
University of Hawaii Environmental Center

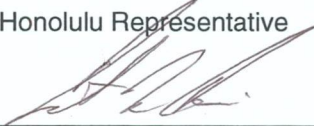
Joseph Blackburn
Maui Representative/LEPC Chair
Maui Fire Department
Maui Representative

Robert A. Boesch
Pesticides Program Manager
Pesticides Branch, Department of Agriculture
Board of Agriculture



John Bowen
Hawaii Representative/LEPC Chair
Consultant and Instructor in Hazardous Materials
Hawaii Representative

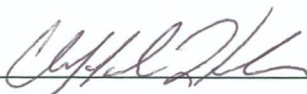
Captain Carter Davis
Honolulu Representative/LEPC Chair
Honolulu Fire Department
Honolulu Representative



Gary Gill
Deputy Director, Environmental Health
Department of Health
Department of Health



Clifford Ikeda
Kauai Representative/LEPC Chair
Kauai Civil Defense
Kauai Representative



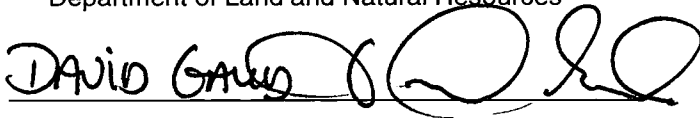
Glen Lockwood
Manager, Emergency Services
American Red Cross
American Red Cross



Sign-In Sheet for HSERC Members Or their Voting Representatives

August 15, 2002

Gary Moniz
Chief of Enforcement
Department of Land and Natural Resources
Department of Land and Natural Resources



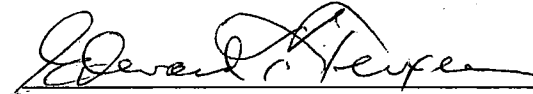
Masayoshi Ogata
Branch Manager
Occupational Health Branch
Department of Labor and Industrial Relations

Genevieve Salmonson
Director
Environmental Quality Control Office
Environmental Quality Control Office

Thomas J. Smyth
Business Services Division
Dept. of Business, Economic Dev. & Tourism
Business, Economic Development & Tourism

Chris Takeno
Hazardous Materials Officer
Department of Transportation
Department of Transportation

Ed Teixeira
Vice Director
Civil Defense Division
Department of Defense



Sign-In Sheet for the August 15, 2002 HSERC Meeting

Name	Organization (If we don't already have this information.)	Phone	Fax	E-mail
Curtis Martin	DOH/HEER	586-4249		
Jim VINTON	TESORO HAWAII	547-3414		
MIKE LATHAM	TESORO / HAWAII	547-3179		m/latham@tesoropetroleum.com
LELAND NAKA	^{HAUL} WPC ^{CONCRETE} OCHA	527-5327		
Latarsha McQueen	MSO	522-8264 x373		lmcqueen@dlt.uscg.mso
Marie Byrd	"	582-8264 x374		mbyrd@dlt.uscg.mso
G/ena Lockwood	"	739-8114 5869104		lockwoodg@hawaii.mso
Tim Shing Chao	HLOSH	586-9090		tin.chao@osha.gov
Dave Hoffman	Tesoro	547-3280		dhoffman@tesoropetroleum.com
CLARENCE A CALLAHAN	DOH	586-0962		ccallahan@cha.health.state.hi.us
Marsha Graf	HEER			
Cynthia Pang	CNR HI	473-		
ED GOMES	HEER			

Sign-In Sheet for the August 15, 2002 HSERC Meeting

Name	Organization (If we don't already have this information.)	Phone	Fax	E-mail
Alan Sugihara	Navy Region Hawaii.			
Tessa Badua-Loosen	FEMA 129	310-627-7185		Tevesita.Badua-loosen@ Fema.gov
Joan Chang	DOH	586 8358		jemchang@ jmail.health.state.hi.us
Tricia Nagatani	DOH-HEER	586-4654		pnagatani@health.state. hi.us
Mike Cupps	HEER			
Terry Corpus	"			
EARL NISHIKAWA	CHEEREN PRODUCES	602-2241		
Beryl Echimoto	HEER			
Liz Galwey	HEER			
Bill Wong	DOH			
Kenneth Chui	FEMA			
Sharon Leonard	HEER			
Clem Sang	SCD			
KATY HO				

BENJAMIN J. CAYETANO
GOVERNOR OF HAWAII



RECEIVED
OFFICE OF THE DIRECTOR
DEPT. OF HEALTH

GILBERT S. COLOMA-AGARAN
CHAIRPERSON
BOARD OF LAND AND NATURAL RESOURCES

ERIC T. HIRANO
DEPUTY DIRECTOR

LINNEL T. NISHIOKA
DEPUTY DIRECTOR FOR
THE COMMISSION ON WATER
RESOURCE MANAGEMENT

STATE OF HAWAII AUG 14 09:49
DEPARTMENT OF LAND AND NATURAL RESOURCES
DIVISION OF CONSERVATION AND RESOURCES ENFORCEMENT
1151 PUNCHBOWL STREET
HONOLULU, HAWAII 96813

AQUATIC RESOURCES
BOATING AND OCEAN RECREATION
COMMISSION ON WATER RESOURCE
MANAGEMENT
CONSERVATION AND RESOURCES
ENFORCEMENT
CONVEYANCES
FORESTRY AND WILDLIFE
HISTORIC PRESERVATION
KAOIOLAWE ISLAND RESERVE
COMMISSION
LAND
STATE PARKS

August 8, 2002

Post-It® Fax Note	7671	Date	8/14	# of pages	1
To	Dennis Shimamura		From	Rabya	
Co./Dept.			Co.		
Phone #	Hand copy to		Phone #	Rabya	
Fax #			Fax #		

Mr. Gary Gill, Deputy Director
State Department of Health
1250 Punchbowl Street
Honolulu, HI 96813

Dear Mr. Gill:

I have asked Mr. David Gaud, DLNR Assistant Enforcement Chief, to attend the next meeting in my place. Assistant Chief Gaud has participated in all forms of emergency preparedness planning for DLNR and has attended many of our interagency discussion meetings.

I need to attend to a family matter that I cannot reschedule. Thank you for your consideration.

Sincerely,

Gary D. Moniz
GARY D. MONIZ
Enforcement Chief

Dennis Shimamoto - HEER

Subject: Re: Agenda
To: "Dennis Shimamoto - HEER" <dshimamoto@eha.health.state.hi.us>
Copies to: ardito.michael@epamail.epa.gov, blackburj001@hawaii.rr.com,
chris_takeno@exec.state.hi.us, cikeda@kauaigov.com, cjung@scd.state.hi.us,
cmartin@eha.health.state.hi.us, dmmaiava@camhmis.health.state.hi.us,
drodrigues@eha.health.state.hi.us, egalvez@eha.health.state.hi.us,
ekni@chevron.com, eteixeira@scd.state.hi.us, glgill@mail.health.state.hi.us,
hazmat@hawaii.rr.com, hcda@scd.state.hi.us, jebowen@gte.net,
jemchang@mail.health.state.hi.us, jth@hawaii.edu,
jvinton@tesoropetroleum.com, kho@eha.health.state.hi.us,
kkawaoka@eha.health.state.hi.us, lmcqueen@d14.uscg.mil,
lnakai@co.honolulu.hi.us, lockwoodg@hawaii.rr.com, masayoshi.ogata@osha.gov,
mcripps@eha.health.state.hi.us, mikulina@lava.net, oeqc@health.state.hi.us,
pangcy@hawaii.navy.mil, shermanp@hgea.org, tcorpus@eha.health.state.hi.us,
tredawson@aol.com, tseelig@co.honolulu.hi.us, tsmyth@dbedt.hawaii.gov,
wperry@eha.health.state.hi.us, David_L_Gaud@exec.state.hi.us
From: Gary_D_Moniz@exec.state.hi.us
Date sent: Wed, 7 Aug 2002 14:16:21 -1000

I have asked David Gaud, DLNR, Assistant Enforcement Chief to attend the next meeting in my place. I need to attend to a family matter that I cannot reschedule. Please call him directly with your questions or concerns. gdm

David Gaud
587-0070

"Dennis Shimamoto - HEER"
<dshimamoto@eha.health.st
jvinton@tesoropetroleum.com, To:
ate.hi.us>

dmmaiava@camhmis.health.state.hi.us,
kho@eha.health.state.hi.us,

08/07/2002 01:58 PM

cmartin@eha.health.state.hi.us,
tcorpus@eha.health.state.hi.us,
mcripps@eha.health.state.hi.us,
egalvez@eha.health.state.hi.us,
wperry@eha.health.state.hi.us,
drodrigues@eha.health.state.hi.us,
kkawaoka@eha.health.state.hi.us,
lmcqueen@d14.uscg.mil,
ardito.michael@epamail.epa.gov,
pangcy@hawaii.navy.mil,
hcda@scd.state.hi.us,
cjung@scd.state.hi.us,

mikulina@lava.net,
ekni@chevron.com,

jemchang@mail.health.state.hi.us,
tredawson@aol.com,
tseelig@co.honolulu.hi.us,
jebowen@gte.net,
blackburj001@hawaii.rr.com,
lockwoodg@hawaii.rr.com,
shermanp@hgea.org,
masayoshi.ogata@osha.gov,
hazmat@hawaii.rr.com,
glgill@mail.health.state.hi.us,
cikeda@kauaigov.com,
jth@hawaii.edu,
lnakai@co.honolulu.hi.us,
oeqc@health.state.hi.us,
tsmyth@dbedt.hawaii.gov,
chris_takeno@exec.state.hi.us,

eteixeira@scd.state.hi.us,

gary_d_moniz@exec.state.hi.us,
ekni@chevron.com,
pangcy@hawaii.navy.mil

cc:

Subject: Agenda

Attached is the agenda for the August 15, 2002 HSERC meeting. Hope to see all of you at the meeting. Aloha.

Dennis Shimamoto - HEER

From: "John Bowen" <jebowen@gte.net>
To: "Dennis Shimamoto - HEER" <dshimamoto@eha.health.state.hi.us>
Subject: Re: MOA
Date sent: Tue, 23 Jul 2002 20:23:07 -0700

Denis, I don't believe that we have such an MOA. But lemme check right away.

I won't be attending the August 15th meeting -- gotta go to teh Mainland for the US Coast Guard.

Cheers!

John Bowen

BENJAMIN J. CAYETANO
GOVERNOR OF HAWAII



RECEIVED
OFFICE OF THE DIRECTOR
DEPT OF HEALTH

HEER/Dennis

GILBERT S. COLOMA-AGARAN
CHAIRPERSON
BOARD OF LAND AND NATURAL RESOURCES

ERIC T. HIRANO
DEPUTY DIRECTOR

LINNEL T. NISHIOKA
DEPUTY DIRECTOR FOR
THE COMMISSION ON WATER
RESOURCE MANAGEMENT

STATE OF HAWAII
DEPARTMENT OF LAND AND NATURAL RESOURCES
DIVISION OF CONSERVATION AND RESOURCES ENFORCEMENT
1151 PUNCHBOWL STREET
HONOLULU, HAWAII 96813

AUG 14 A 9:49

August 8, 2002

AQUATIC RESOURCES
BOATING AND OCEAN RECREATION
COMMISSION ON WATER RESOURCE
MANAGEMENT
CONSERVATION AND RESOURCES
ENFORCEMENT
CONVEYANCES
FORESTRY AND WILDLIFE
HISTORIC PRESERVATION
KAHOOLAWE ISLAND RESERVE
COMMISSION
LAND
STATE PARKS

Mr. Gary Gill, Deputy Director
State Department of Health
1250 Punchbowl Street
Honolulu, HI 96813

RECEIVED
DEPARTMENT OF HEALTH
2002 AUG 19 P 3:58
HEER OFFICE

Dear Mr. Gill:

I have asked Mr. David Gaud, DLNR Assistant Enforcement Chief, to attend the next meeting in my place. Assistant Chief Gaud has participated in all forms of emergency preparedness planning for DLNR and has attended many of our interagency discussion meetings.

I need to attend to a family matter that I cannot reschedule. Thank you for your consideration.

Sincerely,

GARY D. MONIZ
Enforcement Chief

BENJAMIN J. CAYETANO
GOVERNOR OF HAWAII



BRUCE S. ANDERSON, Ph.D.
DIRECTOR OF HEALTH

STATE OF HAWAII
DEPARTMENT OF HEALTH

P.O. BOX 3378
HONOLULU, HAWAII 96801

In reply, please refer to:
HEER OFFICE

LIEUTENANT GOVERNOR'S
OFFICE

'02 AUG -7 A11 :42

HAWAII STATE EMERGENCY RESPONSE COMMISSION
MEETING #47

Thursday, August 15, 2002 from 9:00 a.m. to 12:00 p.m.
Department of Health
919 Ala Moana Boulevard, 5th Floor
Honolulu, Hawaii 96814

AGENDA

- 1) 9:00 Call to Order Gary Gill, Deputy Director for Environmental Health
Opening Remarks
Approval of Minutes from Mtg #46
- 2) 9:15 LEPC Updates John Bowen, Hawaii LEPC Representative
Clifford Ikeda, Kauai LEPC Representative
Joe Blackburn, Maui LEPC Representative
Carter Davis, Oahu LEPC Representative
- 3) 9:45 HMEP Training and Planning Grants Clem Jung, SCD
- 4) 9:55 HMEP Planning Projects Denis Shimamoto, HEER Office
- 5) 10:05 EPA Update Mike Ardito, EPA Region IX
- 6) 10:15 Elec. TIER II Reporting Data System Marsha Graf, HEER Office
- 10:30 Break
- 7) 10:40 Operational Security Briefing Chris McMurray, FBI
- 8) 11:10 Citizen Corps Tessa Badua-Larsen, FEMA
- 9) 11:25 Big Island CHER-CAP Exercise Kenneth Chin, FEMA
- 10) 11:40 Chem-Bio Response Guidelines Ed Gomes, HEER Office
- 11) 11:50 Other Business
- 12) 11:55 Schedule next HSERC meeting

Dennis Shimamoto - HEER

Date sent: Thu, 01 Aug 2002 08:02:25 -1000
To: "Smith, Todd" <Todd.Smith@fema.gov>
From: cjung@scd.state.hi.us (Clement Jung)
Subject: Re: HI SERC Mtg
Copies to: "Chin, Kenneth" <Kenneth.Chin@fema.gov>,
Denis Shimamoto <dshimamoto@eha.health.state.hi.us>

Todd,

I contacted Denis Shimamoto who sets up the HSERC meeting agendas. Ken need to contact Denis with details to put on the agenda. Denis's phone number is (808) 586-4694 and e-mail shown above.

Aloha, Clem

At 10:55 AM 8/1/02 -0400, Smith, Todd wrote:

Good Morning Clem,

Congratulations on completing the Draft After Action Report for the CHER-CAP exercise so quickly. I know it's always difficult to get those types of actions completed after such a large event.

I wanted to let you know that Ken is planning to attend the SERC meeting on the 15th and would like the opportunity to brief on our programs to the committee members. If you could schedule a small block of time, we would appreciate it. Sorry I can't attend, but my schedule has me in AZ that week.

Take care and please note our new address and phone number. Ken Chin (510-627-7122)

~Todd

**Todd Smith
Technological Hazards Program Specialist
FEMA Region IX
National Preparedness Division
1111 Broadway St., Ste. 1200
Oakland, CA 94607-4052
510-627-7235
FAX-7214**

Dennis Shimamoto - HEER

From: "Badua-Larsen, Teresita" <Teresita.Badua-Larsen@fema.gov>
To: "dshimamoto@eha.health.state.hi.us"
<dshimamoto@eha.health.state.hi.us>
Subject: HSERC and Citizen Corps
Date sent: Thu, 25 Jul 2002 12:48:51 -0400
<Teresita.Badua-Larsen@fema.gov>

Dennis, Ken Chin forwarded your email to me regarding a speaker for Citizen Corp. This is one more of those new programs that I am working on. Got permission to attend so please share the agenda with me.

Talk to you soon. Mahalo

Tessa B. Badua-Larsen
National Preparedness Division
FEMA Region IX
1111 Broadway St., Suite 1200
Oakland, CA 94607-4052
510-627-7185 PH
Email: Teresita.Badua-Larsen@FEMA.gov

Dennis Shimamoto - HEER

Date sent: Thu, 01 Aug 2002 10:13:32 -1000
To: "Dennis Shimamoto - HEER" <dshimamoto@eha.health.state.hi.us>
From: cjung@scd.state.hi.us (Clement Jung)
Subject: Re: (Fwd) RE: HI SERC Mtg
Copies to: Kenneth Chin <kenneth.chin@fema.gov>, Todd Smith <todd.smith@fema.gov>

Denis,

I am planning to discuss the exercises at the upcoming HSERC meeting (which John Bowen had committed to at the last HSERC meeting - a WMD/Hazmat tabletop exercise for 2003 and a WMD/Hazmat field exercise for 2004). However, the tabletop exercise for 2003 will be only a Hazmat exercise. For the 2004 not sure at this point if will be a WMD/Hazmat or only a Hazmat field exercise. This 2004 will be a CHER-CAP exercise. Wanted to discuss these exercises with John Bowen at the meeting but you said he will not be at the upcoming HSERC meeting.

It is my understanding that CHER-CAP exercise only pertains to field exercise, i.e., Operation Kalaeloa, and not to tabletop exercises.

Honolulu Police Department is planning to have a WMD field exercise in July 2003 but it is not confirmed and I do not have all the details. This may qualify as a CHER-CAP exercise with Honolulu Police Department (HPD) taking the lead. There are six HPD officer taking the Tabletop Exercise Design Class which is going on right now from July 31 to August 1, 2002.

Clem

At 09:21 AM 8/1/02 -1000, you wrote:

Hi Clem. FYI
----- Forwarded message follows -----

See the messages. Am hoping to attend the HSERC meeting but will be coming late. Would like to bring before the group whether an exercise on the Big Island is still in the works and how it can be made part of a CHER-CAP approved activity

-----Original Message-----

From: cjung@scd.state.hi.us [<mailto:cjung@scd.state.hi.us>]
Sent: Thursday, August 01, 2002 14:02
To: Smith, Todd
Cc: Chin, Kenneth; Denis Shimamoto
Subject: Re: HI SERC Mtg

Todd,

I contacted Denis Shimamoto who sets up the HSERC meeting agendas. Ken need to contact Denis with details to put on the agenda. Denis's phone number is (808) 586-4694 and e-mail shown above.

Aloha, Clem

At 10:55 AM 8/1/02 -0400, Smith, Todd wrote:

Good Morning Clem,

Congratulations on completing the Draft After Action Report for the CHER-CAP exercise so quickly. I know it's always difficult to get those types of actions completed after such a large event.

I wanted to let you know that Ken is planning to attend the SERC meeting on the 15th and would like the opportunity to brief on our programs to the committee members. If you could schedule a small block of time, we would appreciate it. Sorry I can't attend, but my schedule has me in AZ that week.

Take care and please note our new address and phone number. Ken Chin
(510-627-7122)

~Todd

Todd Smith
Technological Hazards Program Specialist
FEMA Region IX
National Preparedness Division
1111 Broadway St., Ste. 1200
Oakland, CA 94607-4052
510-627-7235
FAX-7214

----- End of forwarded message -----Denis Shimamoto
HSERC Coordinator
HEER Office 586-4694 fax586-7537

Dennis Shimamoto - HEER

Subject: **Re: HSERC Meeting**
To: **dshimamoto@eha.health.state.hi.us**
From: **Toby.Clairmont@kp.org**
Date sent: **Fri, 2 Aug 2002 09:26:35 -1000**

Sorry Dennis...I just returned today from Washington DC. My e-mail backlog is a terrible.

Pls consider me for a future meeting - happy to help anyway I can.

Once again, my apologies!

Tob

BENJAMIN J. CAVETANO
GOVERNOR OF HAWAII



BRUCE S. ANDERSON, Ph.D., M.P.H.
DIRECTOR OF HEALTH

STATE OF HAWAII
DEPARTMENT OF HEALTH
P. O. BOX 3378
HONOLULU, HAWAII 96801

In reply, please refer to:
HEER OFFICE
02-182-DS

July 30, 2002

Mr. Dan Dzwilewski
Special Agent in Charge
Federal Bureau of Investigation
300 Ala Moana Blvd. #4-230
Honolulu, HI 96850

Dear Mr. Dzwilewski:

There will be a Hawaii State Emergency Response Commission (HSERC) meeting on August 15, 2002 at 9:00 am on the 5th floor at the Department of Health, 919 Ala Moana Blvd., Honolulu, HI 96814. Commission members are from various State Departments and the Local Emergency Planning Committees (one from each county). Attendees also include members from the private industry and other Federal Agencies. We would like to request Special Agent Chris McMurray to give a talk on the "Operational Security Briefing" at this meeting.

Will you please call Denis Shimamoto, HSERC Coordinator, at (808) 586-4249 or e-mail: dshimamoto@eha.health.state.hi.us on Agent Chris McMurray availability for the HSERC meeting.

Sincerely,

A handwritten signature in black ink, appearing to read "Gary Gill".

Gary Gill
Deputy Director
Environmental Health Administration

Dennis Shimamoto - HEER

Aloha!

Denis, by Aug. 14, I'll send you an EPA update for the Aug. 15 HSERC meeting. I will not be there in person.

Mahalo,

Mike

Dennis Shimamoto - HEER

<dshimamoto@eha.health.s To:
jebowen@gte.net, blackburj001@hawaii.rr.com,
tate.hi.us>
hazmat@hawaii.rr.com, ciked@kauaigov.com,

glgill@mail.health.state.hi.us,

06/24/2002 10:40 AM

lnakai@co.honolulu.hi.us,

cmartin@eha.health.state.hi.us,
Michael
Ardito/R9/USEPA/US@EPA,

kkawaoka@eha.health.state.hi.us

cc:

Subject: HSERC
Meeting Agenda

Do you have any agenda items for the August 15, 2002 HSERC meeting?

Please let

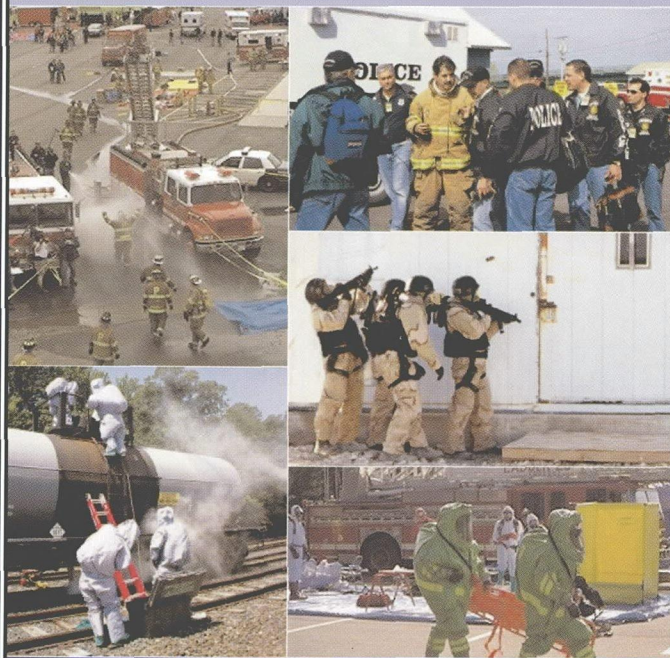
me know by July 22, 2002. Aloha.



OPERATIONS SECURITY FOR PUBLIC SAFETY AGENCIES

SPECIAL OPERATIONS

For Terrorism and Hazmat Crimes



CHRIS HAWLEY ¥ GREGORY G. NOLL ¥ MICHAEL S. HILDEBRAND

Operations Security

Monograph Series

The Interagency OPSEC Support Staff

Our **Vision** is secure and effective operations for all National Security mission activities.

Our **Mission** is to promote and maintain OPSEC principles worldwide by assisting our customers in establishing OPSEC programs, providing OPSEC training, and conducting OPSEC surveys.

Our **Goal** is to be recognized as the leader and preferred provider of value-added OPSEC products and services.

SPECIAL OPERATIONS FOR TERRORISM AND HAZMAT CRIMES®

OPERATIONS SECURITY FOR PUBLIC SAFETY AGENCIES

NOTE: Chapter 3, "Operations Security For Public Safety Agencies" has been adapted and reproduced with permission from the authors by the Interagency OPSEC Support Staff (IOSS) from the textbook entitled, Special Operations for Terrorism and HazMat Crimes®, by Chris Hawley, Gregory G. Noll, and Michael S. Hildebrand. Additional reprints are available from IOSS by calling, 301-982-0323.

For more information on the availability of the text Special Operations for Terrorism and HazMat Crimes call Red Hat Publishing at 800-603-7700 or visit their web site at www.redhatpub.com.

Technical questions concerning this reprint or requests to reproduce copyrighted material from "Operations Security For Public Safety Agencies" should be directed to Mike Hildebrand, email opsec@chesapeake.net.

JUNE 2001

BY: CHRIS HAWLEY, GREGORY G. NOLL, AND MICHAEL S. HILDEBRAND

NOTES

OBJECTIVES

- Define the term Operations Security (OPSEC).
- Explain two reasons why law enforcement and public safety agencies need Operations Security.
- List six basic situations where Operations Security can be of value to law enforcement and public safety agencies.
- Define the terms Threat and Adversary.
- List seven major groupings of Adversaries and explain how these groups may pose a threat to Operations Security.
- List six basic methods Adversaries use to collect intelligence against law enforcement and public safety agencies.
- List the five steps of the Operations Security Process.
- Define Critical Information and provide three examples of information that law enforcement and public safety agencies need to protect.
- List the two components of analyzing a Threat and explain how to determine if an Adversary is a credible Threat.
- List five sources of information for developing a Threat Analysis.
- Define the term Vulnerability Analysis and list three examples of Operations Security vulnerabilities.
- Define the term Indicator and list three examples of Operations Security indicators.
- Describe six basic communications methods that are vulnerable to compromising a law enforcement mission.
- Describe the Risk Assessment process as it relates to Operations Security and list three major factors used in the OPSEC Risk Assessment decisionmaking process.
- Define the term Countermeasure as it used in the Operations Security process and list three examples of countermeasures.

THE WORLD IS CHANGING

NOTES

The world is changing and the public safety community must change with it. If we want to be safe and effective in the future, we must rethink the way we conduct our business. Security needs to be incorporated into the public safety culture and it must become the routine for how we operate, not the exception. In future years, we can be sure that our adversaries will plan operations against us using the most effective intelligence methods and technology. We need to take special precautions and be prepared!

In recent years there has been a great deal of focus on the potential terrorist threat within the United States. While the threat of terrorism in our country is serious, actual incidents are rare. The reality is that there are hundreds of violent criminal acts that occur in our country every day that involve the use of terrorist-like tactics and weapons. Examples include drug-related homicides, school shootings, and sophisticated robberies using assault weapons. These incidents place emergency responders in extreme danger and special security precautions are justified.

In this chapter, we will discuss security issues that face public safety agencies who may be called upon to work as a team in planning for Special Operations or who may work together at the scene of an incident involving Joint Law Enforcement/Fire & EMS/Military Operations. We will provide an overview of the different types of adversaries that represent a potential public safety threat within the United States as well as for federal law enforcement agencies and Department of Defense units who may conduct international operations. We will also introduce the basic concepts of establishing an Operations Security (OPSEC) program and explain how to apply OPSEC for Special Operations at the scene of violent crimes or incidents involving Weapons of Mass Destruction.



STEVE GEORGE ©

FIGURE 3-1 Murrah Federal Building Bombing, Oklahoma City, OK.

NOTES

OVERVIEW OF OPERATIONS SECURITY (OPSEC)**WHAT IS OPSEC?**

Operations Security (OPSEC) is a risk management tool used to deny an adversary (The Bad Guys) information concerning our intentions and capabilities by identifying, controlling, and protecting indicators associated with the planning and execution of law enforcement and public safety missions.

Translation: We have critical information the Bad Guys need to hurt us and we don't want them to get it. OPSEC is a process that helps us deny our adversaries this critical information. OPSEC allows law enforcement and other public safety personnel to look at our operations through the eyes of the adversary. OPSEC can be used to determine how and where critical information related to the safety and success of an operation may be compromised and used against us.

WHY DO WE NEED OPSEC?

The threat to the United States from international organized crime and terrorists is real, it is immediate, and it is evolving with an increasing level of sophistication. Some terrorist's organizations have declared all U.S. citizens legitimate targets of attack at home and abroad. The commitment and ability to carry out this threat has been clearly demonstrated by attacks on the World Trade Center in New York (1993), simultaneous attacks on two U.S. Embassies in Africa (1998) and the Millennium plots to commit terrorists attacks (1999/2000).

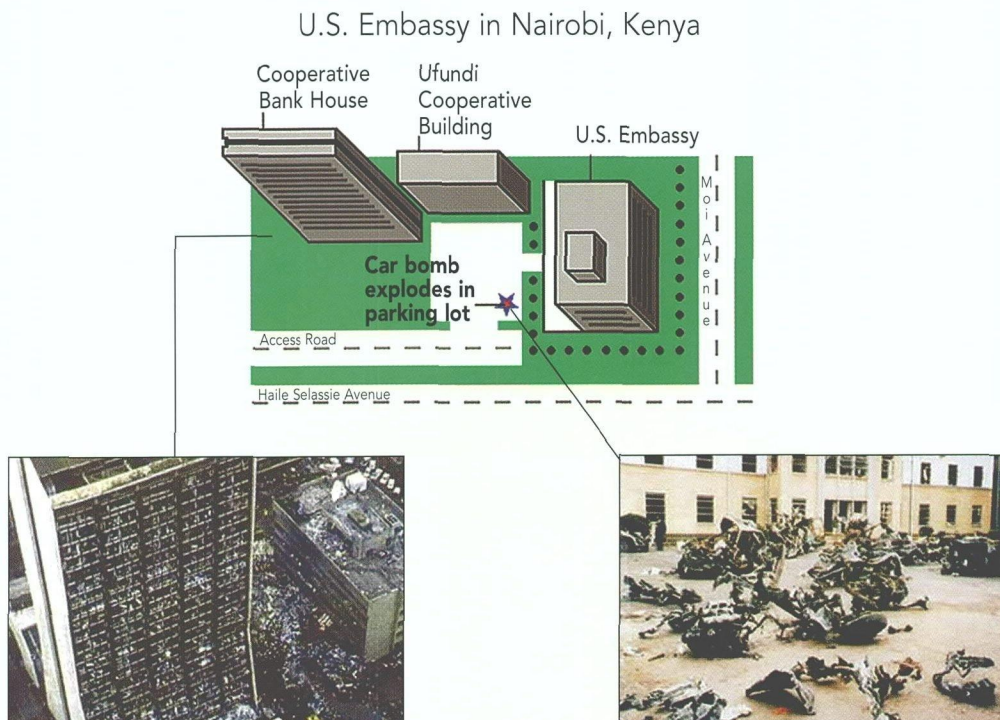


FIGURE 3-2 Car bomb at U.S. Embassy in Nairobi, Kenya.

But the threat to our security goes beyond international terrorists groups who have a base of operation outside our borders. It also includes domestic threats from violent criminals and attacks from cyberspace on our infrastructure and computer networks.

Law enforcement investigations and the testimony of convicted terrorists and criminals have taught us that months of professional and careful planning precede an attack. Criminals and terrorists need information to select their targets and plan their operations. The hard lessons learned from terrorists incidents have taught us that our adversaries are out there right now reading about our operations, watching how we train, and listening to what we have to say about ourselves in public forums.

WHAT CAN OPSEC DO FOR ME?

An effective Operations Security program helps ensure that law enforcement and public safety special operations are conducted with:

- No loss of life or injuries to personnel;
- Safe and secure arrest of the perpetrators;
- Safe and secure collection of evidence;
- Convictions in court;
- Protection of critical information vital to the safety and security of people and information systems.

OPSEC can be applied immediately by public safety agencies to one or more of the following types of situations:

Special Operations Mission Planning—Law enforcement and emergency services Special Operations Teams are increasingly working together in Joint Operations. Examples include narcotics investigations and clandestine drug lab takedowns, interdiction of dangerous cargo, and seizing weapons of mass destruction from smugglers and terrorists. All of these operations require good OPSEC to ensure the success of the operation and the safety of our personnel.

Planning for High Profile Public Events—High profile national level events may include protecting visiting dignitaries, professional sporting events, political rallies, concerts, and parades. These events represent targets of opportunity for terrorists and extremists groups. Integrated multi-agency plans to counter terrorist's threats need an OPSEC component.

Special Operations Training Exercises—Tabletop and field exercises are an important element of preparing for credible threats. But the exercise process can reveal weaknesses and vulnerabilities that we don't want our adversaries to exploit. OPSEC needs to be integrated into exercise planning and design the same way we incorporate safety issues and concerns.

NOTES

Plans and Standard Operating Procedures—Our adversaries are very interested in our strategies, tactics, and methods of operation. When too much information is documented and released to the public we expose our vulnerabilities to a group of people that do not share the same agenda that we have. Good OPSEC procedures help us determine how much information we can share with the public and what we should hold more closely.

Methods, Sources, and Technical Tradecraft—Information concerning our sources of intelligence, and the methods we use to counter a threat, need to be treated as Protected Information. An OPSEC program can help us determine which type of information needs to be protected and help us keep it from our adversaries.

EXAMPLES OF OPSEC PROBLEMS AND CONSEQUENCES

Review the following OPSEC problems and consequences and think about how these problems might relate to the vulnerability of your own organization and community.

OPSEC PROBLEM #1: COMMUNICATING ON THE INTERNET

You are a Hazardous Materials Technician for your public safety organization. You routinely participate in a discussion group on the Internet called HazMat/WMD also known as a One List. Participants on HazMat/WMD are primarily hazardous materials responders from fire and police departments, industry and the military. Anyone may register and monitor the discussion or recall previous correspondence.

Recently, the HazMat/WMD posted a news report concerning the theft of 24 drums of a hazardous material we will call HazMat-X from a trucking company. In the on-line discussion a participant asked the group for any information on the potential use of HazMat-X as a possible terrorist agent.

Over the period of the next week numerous comments concerning this topic were made on HazMat/WMD. One participant provided a detailed description of how HazMat-X was used in industry and its hazards and risks. Another participant provided interesting historical background on World War-I military research and testing of HazMat-X as a potential chemical weapon. The background information included successes and failures of the application of the chemical in different environments. A third participant discussed how a terrorist might actually use the chemical to create panic in a public place. He explained the signs and symptoms that would be produced and the types of medical problems that might be expected from emergency responders.

Another participant described how the HazMat team might respond to such an incident involving HazMat-X .

POTENTIAL CONSEQUENCE

None of the information discussed on the HazMat/WMD One List was classified or protected information. In fact the majority of the information was already available from public sources. Any organized terrorist group could easily assemble the information.

However, what a potential terrorist cannot easily do is get inside the head of public safety responders. By monitoring the discussions on HazMat/WMD under an assumed identity, adversaries would be able to gauge the reaction of the emergency response community to the theft of HazMat-X. They also could gather intelligence on the capabilities of responders, their strengths and weaknesses, types of protective equipment available, and monitoring capabilities. They could even learn the opinion of the HazMat community concerning which types of targets would be easy to access and their vulnerabilities.

OPSEC PROBLEM #2: LAW ENFORCEMENT SENSITIVE INFORMATION

Your Training Academy has been asked to conduct a 40-hour Hazardous Materials training program specifically targeted towards the needs of federal law enforcement officers who are involved in both special operations and crime scene investigations. On the last day of the class, a student who is a Special Agent approaches the Lead Instructor and advises that she must leave the class early. She tells the instructor that the class has been great, but she is involved in a tactical operation that is being conducted early Saturday morning.

After class, the Lead Instructor receives a phone call on his personal cell phone from another Fire Officer in a neighboring jurisdiction inquiring on his availability to provide specialized terrorism training for their command officers. The phone conversation goes something like this:

"Hey Chris, I hear there is some kind of special operation going down with the feds in your area this weekend....is your HazMat Team involved?"

Chris replies, "That's news to me, nobody told me anything about it. I'll check around and call my friends with the police department."

Chris then uses his personal cell phone to call his friend Phil on his personal cell phone. (Phil is a member of the Police Department SWAT Team.) The conversation goes something like this:

"Hey Phil, this is Chris. I heard from a friend of mine who heard it from a Special Agent in his HazMat class that the feds are planning some kind of tactical operation or take-down in our area Saturday morning. Do you know anything about it?"

POTENTIAL CONSEQUENCE

In this example the Special Agent used poor judgment and bad OPSEC by revealing information concerning her special operation to the Training Instructor. Remember that clearance plus "need to know" equals access to special information. The information shared with the Instructor by the Special Agent should have been treated as "Law Enforcement Sensitive" information by the Instructor and not shared with other colleagues who had No Need To Know this information. When the Lead Instructor casually passed on the information to his peers, he placed the law enforcement mission and possibly the lives of law enforcement officers at risk.

Unfortunately, "Bad Guys" sometimes have the capability to monitor cellular telephones and radio communications. Through effective intelligence gathering techniques, the "Bad Guys" can often determine who are the members of the Police SWAT Team. By monitoring cell phone traffic and placing surveillance on key SWAT Team members, it is possible to determine future operations. In this scenario, the timing and level of detail revealed in the telephone call could easily provide an early warning for the bad guys.

OPSEC PROBLEM #3: LOCAL EMERGENCY PLANNING COMMITTEE

As the county Emergency Management (EM) Director, you serve as an Executive Committee member for a Regional Counterterrorism Task Force that includes members from the law enforcement, fire, emergency medical services, hospital and public works organizations. An initial priority of the Task Force is to conduct a Threat Assessment and identify and prioritize the most likely targets of a terrorist attack.

After a recent meeting of the Local Emergency Planning Committee (LEPC), the EM Director had a casual conversation with several members of the LEPC, including a community activist and a television reporter who have been long-time and trusted members of the LEPC. Several days later, an article appears in the weekly edition of the local newspaper stating that your community is evaluating its preparedness for terrorism events and includes a list of possible targets throughout the region. Remarkably, the list closely mirrors the initial list that was developed by the Regional Counterterrorism Task Force.

POTENTIAL CONSEQUENCE

In this example the Emergency Manager used poor judgment and bad OPSEC by revealing information that was being developed by the Counterterrorism Task Force. In many areas, Regional Task Forces are being used as a vehicle for bringing many diverse groups together that may have a shared mission in preparing for and responding to terrorism events. While law enforcement personnel often have a basic understanding of the need for security, the same level of understanding is often lacking or absent in public safety organizations that do not routinely deal with law enforcement issues.

One could argue that the information discussed by the EM Director is probably already known by most criminals and terrorist groups. However, when the lists of likely targets is combined with information that is often easily available through the Freedom of Information Act–FOIA (e.g., chemical inventories, environmental permits, EPA Risk Management Planning, etc.), it can provide the "Bad Guys" with a great deal of intelligence with very little effort and risk on their part. Members of the Local Emergency Planning Committee should receive a basic OPSEC Awareness orientation to help them understand the importance of controlling critical information.

OPSEC PROBLEM #4: CONTROLLING OFFICE ACCESS AND TRASH

The Regional Drug Task Force has requested that the fire department support a special operation it has been planning for over six months. The Chief of the Department has assigned a senior fire officer (you) to attend a Task Force Planning meeting.

At the initial meeting it is learned that the Drug Task Force is planning a simultaneous take-down of two PCP labs in your jurisdiction. The Task Force is requesting fire department support for both emergency medical services (EMS) and decontamination. Due to operational security, the date and time of the raid has not been revealed to the Fire Department.

During the meeting, a State Police Detective provides a briefing on the types of chemicals and other hazards that should be expected by the Fire Department. The Task Force Leader specifically requests that the Fire Department be prepared to help with emergency decontamination and EMS support.

The day after the initial Task Force meeting, the Fire Department representative prepares a memorandum outlining the key points from the briefing, the names of the Task Force members, and the chemicals of concern that are expected to be found in the clandestine laboratories. This officer goes through several hard copy drafts before he e-mails his memo to the HazMat team shift officers. He goes home leaving the drafts in the trash can.

POTENTIAL CONSEQUENCE

Manufacturers of illicit drugs and chemicals know that public safety HazMat response teams are often called upon to support police tactical operations for clandestine drug lab take-downs. This support can include emergency medical services, chemical protective clothing, air monitoring decontamination, and logistics.

Drug dealers also know that Fire Departments can be easy targets for intelligence. They have many informants in the community and can use them to exploit vulnerabilities. For example, informants may be working on the cleaning staff that has the contract for the City Office Building. If an informer worked on the cleaning staff in your building they would certainly scout the offices for useful information. Looking through trashcans and "dumpster diving" is a standard intelligence gathering method.

If draft documents were improperly discarded in the office trash, an informer could pass on important information to the drug dealers. If they were tipped off about the Task Force's activities, the labs would probably be abandoned in place. No arrests would be made and months of complex and expensive police work would be wasted.

THREATS AND ADVERSARIES

WHO IS A THREAT?

For purposes of this text, a threat is any individual, organization, or country that has the intent and technical capability to attack us by exploiting our vulnerabilities. The THREAT could be against people, property, or the critical information we need to ensure the safety and success of our mission. Anyone who represents a threat to our personal safety or our operations should be treated as an ADVERSARY.

WHO IS AN ADVERSARY?

Operations Security professionals define an adversary as anyone who may be collecting information about us and our organization and intends to use this information to either defeat our operations or plan an attack against us.

It should be kind of obvious that if we: 1) Know who our adversaries are, and; 2) Know their intentions and capabilities, we can intelligently estimate the threat. We can also take steps to eliminate the threat or reduce the impact the threat might have on our operations. Later in this chapter we will explain how to evaluate a potential threat by conducting a Threat Assessment.

TYPES OF ADVERSARIES

Adversaries have different types of goals, objectives, motivations, and capabilities. To meet the needs of the target audience for this textbook, we have organized adversaries into seven major groupings. These include:

- International Terrorists Groups
- Criminals
- Organized Crime and Drug Trafficking Groups
- Domestic Militia Groups
- Extremist Groups and Cults
- Foreign Intelligence Agencies
- Hackers and Crackers

INTERNATIONAL TERRORISTS GROUPS

NOTES

Terrorism is a pre-meditated, politically motivated act of violence perpetrated against non-violent targets. Clandestine agents usually carry out terrorism and the acts of violence they commit are intended to influence a large audience.

The U.S. State Department currently lists about 29 different groups that are engaged in Terrorist Activity. The greatest threat in the United States from terrorist groups are Islamic Fundamentalists. Visit the State Departments web site at www.state.gov for a detailed summary of these terrorist groups and their history.

U.S. State Department Legal Definition of Terrorist Activity

The term "terrorist activity" means any activity which is unlawful under the laws of the place where it is committed (or which, if committed in the United States, would be unlawful under the laws of the United States or any State) and which involves any of the following:

- (I) The hijacking or sabotage of any conveyance (including an aircraft, vessel, or vehicle).
- (II) The seizing or detaining, and threatening to kill, injure, or continue to detain, another individual in order to compel a third person (including a governmental organization) to do or abstain from doing any act as an explicit or implicit condition for the release of the individual seized or detained.
- (III) A violent attack upon an internationally protected person (as defined in section 1116(b)(4) of title 18, United States code) or upon the liberty of such a person.
- (IV) An assassination.
- (V) The use of any:
 - (a) biological agent, chemical agent, or nuclear weapon or device, or
 - (b) explosive or firearm (other than for mere personal monetary gain), with intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property.
- (VI) A threat, attempt, or conspiracy to do any of the foregoing.
- (iii) ENGAGE IN TERRORIST ACTIVITY DEFINED.-Means to commit, in an individual capacity or as a member of an organization, an act of terrorist activity or an act which the actor knows, or reasonably should know, affords material support to any individual, organization, or government in conducting a terrorist activity at any time, including any of the following acts:

NOTES

- (I) The preparation or planning of a terrorist activity.
- (II) The gathering of information on potential targets for terrorist activity.
- (III) The providing of any type of material support, including a safe house, transportation, communication, funds, false identification, weapons, explosives, or training, to any individual the actor knows or has reason to believe has committed or plans to commit a terrorist activity.
- (IV) The soliciting of funds or other things of value for terrorist activity for any terrorist organization.
- (V) The solicitation of any individual for membership in a terrorist organization, terrorist government, or to engage in a terrorist activity.

In recent years, public safety agencies have been exposed to much new training and information concerning the threat of terrorism. The subject has been treated as if this problem just materialized over the last few years. But the fact is that terrorism has been a threat to the United States since its birth and has been a tool used in society for thousands of years. What is different today is that the terrorist's strategy and tactics has evolved to include Weapons of Mass Destruction (WMD).

Terrorists have traditionally avoided "killing in excess" in order to gain attention from the people or organizations they oppose, while at the same time, seeking to gain support from a certain segment of society. Until the 1990's, the unwritten doctrine of terrorism was that they wanted a lot of people watching and not very many people dead. The emphasis was on bringing focus on the cause of the terrorist group. Killing too many people at one time could produce a negative effect in public opinion.

In the past, the tools of the terrorist's trade included guns, letter bombs, and the occasional package or car bomb. Historical acts of terrorism were simple events that did not need a great deal of resources and technical capability to carry out the operation. All that was required was the motive and commitment to follow through with the crime. Likewise, the plans needed to execute a terrorist operation were relatively simple; e.g., kidnap somebody important; hijack an airliner to another country and let everyone go; call the police and warn them a car bomb will be detonating at a specific time and place, so the area can be cleared, etc.

A more violent breed of terrorist has evolved since the 1980's. Terrorist groups are playing by a new rulebook that doesn't have too many rules in it. Instead of taking an Ambassador as a hostage to achieve a specific demand, the terrorist takes the entire Embassy and kills the hostages. Instead of sending a letter bomb to a government official and killing the target, an entire building is

blown up killing hundreds of people, including innocent children. Instead of hijacking an airliner, the entire aircraft is blown up over a populated area.

In addition to becoming more ruthless, terrorists' organizations are developing better technical capabilities and their plans are becoming harder to detect. According to the U.S. Central Intelligence Agency (CIA), several international terrorists groups who have adopted an anti-American doctrine have decentralized their leadership, making it harder for U.S. Intelligence and federal law enforcement agencies to identify and disrupt their operations before they commit violence.

Terrorists groups are also employing increasingly advanced Improvised Explosive Devices (IED's) and are using strategies such as simultaneous attacks on different targets. This is evidenced by the fact that the number of people killed or injured in international terrorist attacks rose dramatically in the 1990s, despite a general decline in the number of incidents. Another factor effecting terrorist strategy is that as we have increased security around government and military facilities, terrorists have sought out "softer" targets that provide better opportunities for mass casualties with less risk.

International terrorist networks are also using the rapid expansion in information technology to improve their capabilities to carry out terrorist acts. The same technologies that allow Americans to search out information on the Internet from anywhere in the world also enables terrorists to gain access to U.S. owned and controlled Websites and e-libraries. Terrorists routinely use the Internet to raise money, spread their beliefs, find recruits, and plan operations. Terrorist groups are also actively searching the Internet to acquire information to develop more deadly capabilities for chemical, biological, radiological, and even nuclear attacks. In 1998, Usama bin Ladin even declared acquisition of Weapons of Mass Destruction technology a "religious duty."

CRIMINALS

While the United States is one of the safest places to live, there is a long and growing list of domestic criminals who represent a threat to our economy and safety. As an adversary, criminals are distinguished from terrorists by their motivation and objective. Criminals are primarily motivated by personal revenge or financial gain. They may also be driven to commit a violent crime by psychological pathologies.

Criminals are usually not committed to any particular ideology and it is sometimes difficult to determine if they are motivated by political or basic criminal intent. For example, some criminals have tried to extort money from governments or corporations using a Bomb Threat while making political demands. The intent all along was to simply extort money.

The most serious threat to public safety from individual criminals is the use of improvised and commercial explosives as a weapon of mass destruction. The most striking example is the Oklahoma City bombing where one individual murdered 168 innocent people using an improvised ANFO bomb.

NOTES

Another significant threat involves criminals who use accelerants, corrosives, or other hazardous materials in the commitment of their crime. They may also use these materials as a means of seeking revenge or for masking the real objective of their crime; e.g., an accelerant may be used to burn a home to cover up a murder or burglary that went bad.

Bank robbers are using sophisticated weaponry, and are becoming increasingly more brazen about their criminal activity. They are using heavier weapons and are better protected than the police. For example, on February 23, 1997 two men robbed a bank in Los Angeles wearing heavy body armor. Both men literally walked down the street gunning down police officers and civilians, all the while taking shots from the police. Their body armor and heavy weaponry allowed them to walk freely for a long period of time. When cornered one robber shot himself, and the other died in a close quarter gun battle with the SWAT team.

ORGANIZED CRIME AND DRUG TRAFFICKING GROUPS

Drug traffickers are the most significant direct and indirect organized crime threat to U.S. public safety agencies. Drugs produced in foreign countries routinely find their way onto U.S. streets and the large sums of cash generated by illegal narcotics sales help fuel violent crime that threatens the lives of public safety officers. Drug Dealers are usually armed well and have shown that they will not hesitate to use weapons indiscriminately.

International drug organizations are becoming more capable and efficient at gathering intelligence on U.S. law enforcement. They routinely use sophisticated intelligence techniques, which require that we conduct our operations using the best Operations Security practices.

According to the Central Intelligence Agency, Colombia, Bolivia, and Peru supply all of the cocaine consumed in the United States. Colombia is the center of the global cocaine industry and is the home of the largest coca growing, coca-processing, and trafficking operations in the world.

Nearly all of the world's opium production is concentrated in Afghanistan and Burma. Production in Afghanistan accounted for 72 percent of illicit global opium production in 2000.

Locations like Columbia, Burma, and Afghanistan seem like far away exotic places but responders need to recognize that the drug threat in these countries is increasingly intertwined with other terrorists threats and capabilities that effect Americans. For example, according to the CIA, the Taliban regime in Afghanistan, which allows Usama Bin Ladin and other terrorists to operate safely on its territory, also encourages and profits by the drug trade. Some Islamic extremists view drug trafficking as a weapon against the United States and drugs are seen as a source of revenue to fund terrorists operations.

DOMESTIC MILITIA GROUPS

The Militia Movement has primarily evolved since the 1990's and its growth has been fed by issues like gun control and federal land use as well as the incidents

at Ruby Ridge (1992), Waco (1993), the Montana Freeman Standoff (1996).

There is no official definition of a Militia Group, but they have two common characteristics: 1) The group possess and uses firearms, and, 2) Conducts or encourages participation in paramilitary training. Examples of U.S. based Militia Groups include the Aryan Nations Organization, the Christian White Supremacists, and the Christian Patriots.

Some Militia members have a history of strong personal beliefs in anti-Semitism, survivalism, or neo-nazi extremism. While this is somewhat disconcerting, Militias have not evolved as a major threat to public safety. Historically, members have limited their activity to anti-government rhetoric which ranges from protesting government policies to advocating overthrow of the government.

There are some radical elements of Militia Groups that are capable and willing to commit violence against law enforcement, civilian, and military targets. In recent years, members of Militia Groups have been involved in a number of hate crimes that have targeted Gays, African Americans, and Jews. These heinous crimes have included torture deaths of selected ethnic and religious group members, church burnings, and bombings of Abortion Clinics.

Some of the more extreme and violent members of Militia Groups form their own splinter groups or become rogue members and commit acts of violence independently of the group. They are sometimes banned from the militia by its members because their personal philosophy and beliefs are seen as being "too extreme and violent" for the mainstream members of the group.

EXTREMIST GROUPS AND CULTS

FAR RIGHT EXTREMISTS

The Far Right Extremist Groups cover the spectrum from White Supremacists and Neo-Nazi's to Christian Identity Groups. Many members of these groups tend to believe in conspiracy theories. They believe that they have moral superiority over other people who are not members of their group and think that most outsiders are villainous and immoral. A few extremists groups advocate terrorism and see violence as a "sacramental act" or a divine duty to God.

ENVIRONMENTAL AND ANIMAL RIGHTS EXTREMISTS

There are many environmental and animal rights groups in the United States who exercise their rights under the Constitution and legally influence the legislative process by organizing public protests, exercising freedom of speech, and influencing policymaking with governments and corporations. Some disillusioned members of legitimate environmental organizations have formed radical splinter groups that have turned to violence and criminal acts to further their cause.

Since 1997 several of these environmental and animal rights groups have been responsible for over \$40 million in damage to public property by committing arson. Typical targets for environmental extremists have included energy

NOTES

and power companies, recreational facilities, and corporations involved in land development. Targets for animal rights extremists have included research and development facilities that use animals in medical research as well as establishments that process animals as a food source.

Environmental and animal rights extremists typically organize, plan, and execute their operations independently through the Internet. There are numerous environmental and animal rights oriented web sites that outline the goals and objectives of these organizations as well as suggest specific targets and tactics. This includes sabotage and arson. See Figure 3-3.



BATF®

FIGURE 3-3 Bureau of Alcohol Tobacco and Firearms Special Agents and accelerant detection canine search Vail, Colorado ski resort destroyed by arson on October 19, 1998 by environmental extremists. Damages \$12 million.

CULT GROUPS

According to the FBI, there are over 1,000 cults operating in the U.S., and very few represent a credible threat to public safety and law enforcement. Most Cults believe in some kind of biblically-based doomsday scenario.

Cult groups that have a predisposition toward violence have three social-psychological components that psychologists refer to as the "Lethal Triad." These include a group that: 1) Is dependent on its leader to make the key decisions; 2) Is isolated from the critical thinking of the outside world, and 3) Projects its anger for the group's problems at the outside world.

Cult Groups that represent the greatest threat to law enforcement and public safety from violence are those that: 1) Believe they play a special, elite role in some aspect of biblical prophecy; e.g., the endtime (Armageddon); 2) Believe violent offensive action is needed to fulfill their prophecy; and 3) Take steps to attain their beliefs.

There should be no doubt that some extreme cults can be fully committed to their cause. History can point to numerous recent examples of the extent of their extremist principles. Examples include:

- The 1997 Heaven's Gate Cult that killed 39 of its members by suffocation and drug-induced suicide. The Cult's leader convinced the group to take their own lives so that their spirits could ride on a spaceship to heaven that they believed was hiding behind the Hale-Bopp Comet.
- The 1993 shoot-out in Waco, Texas at the Branch Dividian Complex. This armed confrontation resulted in the death and injury of law enforcement officers and the death of all cult members in a raging fire.
- The 1978 Reverend Jim Jones's systematic Kool Aid poisoning of over 900 people and the murder of a U.S. Congressman in Guyana (1978).

FOREIGN INTELLIGENCE AGENCIES

The average American's perception of intelligence work is formed from spy novels and movies. These fictional plots have secret agents plying their trade-craft using "gee whiz" state-of-the-art spy gadgets under deep cover. These stories are largely fiction. The reality is that about 95% of the information gathered by foreign intelligence agencies against the United States comes from open source, unclassified information, not through what most of us would consider traditional spy techniques.

Foreign intelligence agencies routinely read what Americans write, listen to what we say, and watch what we do. Foreign intelligence agencies are particularly interested in gaining access to information about our technology so that they can gain a competitive edge on the United States. Consequently, U.S. corporations and their employees are routine targets for information.

The largest threat to our domestic public safety from foreign intelligence agencies comes from hostile countries that have adopted a doctrine of developing Weapons of Mass Destruction capability for military or terrorist purposes. It should be fairly obvious that countries that have a history of nation-sponsored terrorism are deeply interested in our Domestic Preparedness capabilities and our ability to protect and defend our citizens against a WMD attack. In an indirect way, law enforcement and public safety agencies can become a target of foreign intelligence collection, especially if they are involved in WMD counter-terrorist training or in developing technical countermeasures.

HACKERS AND CRACKERS

Hackers are individuals or groups of individuals who break into government and corporate computer systems to embarrass the owner of the system or to plant a virus intended to disrupt the business of the organization. Very few Americans have not been affected in some way by the work of hackers.

Hackers are usually motivated by the sport and intellectual challenge of breaking into what is supposed to be a secure data base. They receive a great

NOTES

deal of satisfaction from the publicity they gain in the news media or through the acknowledgement and praise they receive from the clandestine hacker community. When caught, hackers often claim that they never really had any intent to harm anyone. Their real purpose was to simply demonstrate the computer systems vulnerability to exploitation by the "real" criminals.

Crackers are individuals who hack into a computer system with the specific intent of stealing or damaging information. Crackers can be professional criminals who have specific intent to gain access to financial information such as credit card and personal data that can either be used personally by the cracker or sold to other criminals.

Terrorist groups, organized crime syndicates, or foreign intelligence agencies may employ crackers. Their motive may be to steal technical data, plans and procedures, or to gain access to unclassified communications via e-mail transmitted on the Internet. Information obtained by crackers can be used in achieving the goals and objectives of the organization they work for, or the information may be sold to another criminal or terrorist organization.

OTHER TYPES ADVERSARIES

In addition to the active adversaries described above, you should be aware that there could be other individuals who can pose a threat to your operations and should be considered an Operations Security risk. They may include:

Disgruntled Employees—People that work within your organization who have access to critical information such as plans and procedures or know your vulnerabilities. They may intentionally leak information to the media to embarrass someone within the organization. They may be motivated to take these extreme steps by anger; e.g. on-the-job harassment, failure to receive a promotion, etc.

Dishonest Employees—While this is rare in public safety agencies, a dishonest employee can become an adversary by intentionally revealing sensitive information about a law enforcement operation to criminals. These individuals have usually developed a substance abuse or behavior problem.

HOW ADVERSARIES COLLECT INTELLIGENCE

To become effective OPSEC practitioners, we have to look at our own operations through the eyes of the adversary. As an example to illustrate this point, let's change rolls and imagine that we are a terrorist organization instead of a law enforcement or public safety organization. Let's also assume that our terrorist cell has the motive and capability to carry out an operation in a U.S. city.

We have selected your city for an attack during a major public event. Our general plan is to:

- 1) Take hostages inside of a government office building;

- 2) Plant explosive devices at the primary entrances of the building to block rapid entry of Special Operations units;
- 3) Hold off the police in a defensive perimeter as long as possible to obtain media coverage, while we negotiate the release of a terrorist leader held in a federal prison.
- 4) We are prepared to die to further our cause. The Police are our primary adversary, and within the Police organization, we have identified the Special Operations Unit as a major threat to our operation.

To effectively plan our operation we will need good intelligence. Once we have selected the target building, we will want to know the How, Who, When, What and Where of the Police Department's Special Operations Unit. Our planning cell will specifically want to know:

1. **HOW** many people are on the Special Operations team and how they are organized? We would also want to know how the Police operate at the tactical level for a hostage situation. We would want to obtain copies of their Standard Operating Procedures.
2. **WHO** are the leaders of the Special Operations Unit and what are the names of the team members?
3. **WHEN** does the Special Operations Unit train and conduct exercises? We would want to observe how they train.
4. **WHAT** type of intelligence capability does the Special Operations Unit have and what type of secure communications and tactical gear do they carry? Do they have Explosives Ordnance Disposal capability? If so, what type of countermeasures do they use?
5. **WHERE** does the Special Operations team train and exercise? Where does the team receive back up from? The terrorist would probably want to know the same types of information about your mutual aid teams as well.

OK, we are the Good Guys again. Let's think about this example for a moment. As you read through the list of information the terrorists wanted to know, you may have developed the impression that they would have to have an inside informer to gather that much information. While an insider acting as a "spy" would be very useful, the Bad Guys could probably get most of the information they needed to plan their operation by careful observation and researching open source material. If we did not have a good OPSEC program in place, it actually might be very easy. Let's take a look at how the terrorists might get the information they need.

INTELLIGENCE METHODS USED BY ADVERSARIES

Criminals and terrorists may take weeks or months to collect the information they need to plan an operation. They usually use the easiest methods and

NOTES

sources of getting information early in the planning stages to minimize the risk of their operation being compromised. If we understand how information can be collected by the Bad Guys and used against us, we can take steps to protect the information that we determine is critical.

The following sources and methods are examples of common ways criminals and terrorists collect intelligence:

- Open Source Research
- Public Domain Technical Reports
- People
- Communications
- Photography
- Trash

OPEN SOURCE RESEARCH

Open Source Intelligence (OSINT) is a widely used information gathering technique that uses legal methods from publicly accessible sources. The three most basic sources of information are:

Freedom of Information Act (FOIA)—This United States Statute was enacted in 1976 and allows anyone to request information from the federal government if information was produced by a federal agency.

There are a number of exemptions under FOIA that protect classified national security information and sensitive trade secret proprietary information. However, any information not covered by an exemption can be obtained by any U.S. citizen, corporation, and any government agency. Many people are surprised to learn that FOIA also allows any foreign government or foreign national to file a FOIA request with any U.S. federal agency. Even a convict in prison can file a FOIA request for information. In fact, prisoners have a lot of time on their hands and often exercise their rights under FOIA.

Anything that conveys information and is under the control of a federal agency is covered by FOIA unless one of the exemptions applies. This includes hard copy and electronic documents, e-mail, videos, and audiotapes. Federal law enforcement and intelligence agencies routinely receive thousands of requests for information under FOIA that are protected by one of the exemptions. If the FOIA request is refused on the grounds of an objection, any citizen has the right to appeal a refusal to release information through the judicial system.

If you are a federal law enforcement or public safety agency that receives federal funding through a federal agency for Special Operations equipment, planning, training, or exercises, you should become familiar with the pros and cons of FOIA and how information releases to the public can

effect the security of your operations. You should also know whether your critical information is protected under FOIA exemptions and what steps to take to prevent an unauthorized release.

Internet—In the age of Information Technology distance is no longer an obstacle to criminals, and borders no longer apply. Prior to 1989 very few Americans had access to the Internet and even fewer people really understood what the Internet's capabilities were. That was then, this is now.

What used to take months to research in 1990 can now be done in one day. Unfortunately, the Internet has evolved so quickly that very little consideration has been given to security issues. Do we really want children to have access to Web Pages that tell them how to make a pipe bomb? Do we really want terrorists to have access to Web Pages that describe the worst case scenarios for every chemical plant in the United States?

The good and bad news about the Internet is that everyone that wants access can get it for free through their local public library. Powerful search engines make it easy to gain access to government and corporate web pages where an unbelievable amount of information can be downloaded. Some security professionals jokingly refer to the Internet as the "Great American Information Giveaway." Here are a few weaknesses of the Internet that criminals and terrorists exploit to learn more about you and your organization:

- **Web Pages**—Government agencies and corporations are proud of their accomplishments and use Web pages to sell themselves and make it easy to access information. Unfortunately there is too much sensitive information on many web pages that can be used against us. If your organization has a Web page you should take a second look at it through the eyes of the adversary. How much information do you really need to have on a web site?
- **Chat Groups and One Lists**—Chat Groups allow anyone to sign on and join in a discussion about issues of common interests. One Lists usually require the participant to sign on and register. In theory, the list is only accessible to certain personnel. The participant must use a password to gain access to post a listing.

People that manage One Lists for public safety audiences do so as a public service and have good intentions. However, they do not have the time, expertise, or resources to do background checks or confirm the identity of the participants.

Almost anyone can assume an alias and join a One List. You should not be surprised that criminals, terrorists, and foreign intelligence agents can easily join Chat Groups and One Lists. Law enforcement and public safety personnel sometimes naively share too much information about their capabilities, fears, and vulnerabilities on One Lists. Anyone who has access can check the historical archives of a One List and read all of the past exchanges of information.

NOTES

- **E-Mail**—There is some reasonable and reliable level of privacy when using e-mail, but privacy is not the same thing as security.

E-mail is not a secure method of communications and can be easily accessed by hackers, read by your service provider, or compromised by a virus. Likewise, documents and photos attached to email are equally unsecure.

Public Domain Technical Reports—There are millions of hard copy and electronic reports available in the public domain through libraries and research services. Powerful search engines make sorting the titles and narrowing the fields of information easy. Try doing a word search for the word explosive and see how many hits you get.

PEOPLE

Human intelligence (HUMINT) relies on people to watch, listen, document, and report on specific operations. People doing HUMINT work may receive general assignments to collect information or be tasked to report on a specific type of activity, e.g., to call a specific cell phone number every time they see a specific person leave a specific building.

HUMINT can involve the use of informers, trained foreign intelligence agents, trusted agents, or a combination of these resources.

- **Informers**—Informers are paid by criminals in cash or drugs to obtain and pass on specific information about a target. Examples of informers may include people who work in the service industry who have routine access to your work area, or hang out at restaurants and bars frequented by you and members of your team.
- **Foreign Intelligence Officers and Agents**—Intelligence officers are professional "spooks" trained in the art and science of intelligence techniques. Intelligence "Agents" are the people who are recruited locally to work for Intelligence Officers.

Most foreign Intelligence Officers and Agents are capable of conducting covert operations, but why take the risk of getting caught? With some good research and detective work they can easily collect lots of unclassified information using open source techniques!

- **Trusted Agents**—Trusted Agents operate covertly much like informers, however, they are not motivated by compensation and are usually not paid for their services. They may cooperate with a foreign government or an extremist organization for political, religious, or patriotic reasons. Trusted Agents provide information because they believe they are doing the right thing (they just aren't).

COMMUNICATIONS

Communications or "Signals Intelligence" (SIGINT) is an intelligence technique that monitors radio, landline telephone, cellular telephone, FAX, and e-mail transmissions using a variety of electronic eavesdropping methods. A simple

example of a SIGINT technique is the use of a Scanner Radio to monitor unsecure police and fire department radio communications.

There is a wide variety of SIGINT eavesdropping hardware that can be legally obtained on the open market. Equipment quality ranges from Radio Shack to military. This equipment can be put to illegal use by criminals and foreign intelligence operatives to monitor telephone and e-mail conversations of U.S. law enforcement agencies using unsecure communications.

PHOTOGRAPHY

Photography or "Imagery Intelligence" uses still and video photography to collect information that can be used to assemble an amazing variety of information about your organization and the community you are sworn to protect. The old saying that a "picture is worth a thousand words" is certainly true. Photographs can be studied over and over again, blown up and enhanced for detail, and even modified and super-imposed on another image such as a map for comparison.

Photographs of equipment and personnel can be obtained through close-in covert surveillance or through open-source public events such as training exercises, hardware displays, and public demonstrations of your capabilities. Other sources include media coverage of actual operations, or downloadable photos available from your web site over the Internet.

Satellite photographs of many public buildings and attractions can be downloaded for free off the Internet with incredible resolution. Anyone can purchase high-resolution intelligence quality satellite photographs of major public and government buildings over the Internet from companies that specialize in satellite and aerial photography.

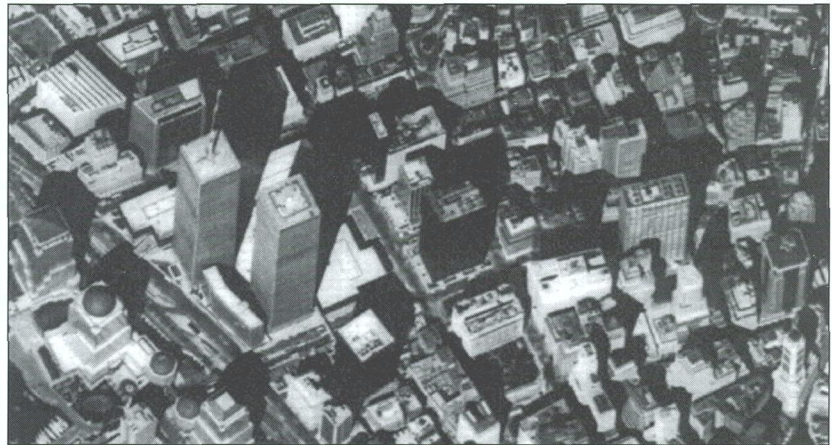


FIGURE 3-4 Satellite photo of World Trade Center.

TRASH

Trash Intelligence is pretty much self-explanatory. Anyone who has access to your office trash can or your building's dumpster can tap a potential gold mine of information about your operations. This might include draft operational plans, names and telephone numbers of key people, old copies of training manuals, critiques and lessons learned, or standard operating procedures. What criminal or terrorist wouldn't love to have this information? Unless you have

NOTES

good OPSEC and have implemented a trash management program, all the Bad Guys have to do is wait for you to go home and go Dumpster Diving.

THE OPSEC PROCESS

By this point you are probably getting a little paranoid. Good! Hopefully we have convinced you that you need to adopt an OPSEC program and run your operations differently in the future. In this section we will take a detailed look at the key components of an effective OPSEC program and discuss some practical security tips and countermeasures that can be implemented to deny an adversary access to critical information.

The OPSEC process consists of five different steps. These steps are:

- Identifying Critical Information
- Conducting a Threat Analysis
- Performing a Vulnerability Analysis
- Assessing Risks
- Applying Countermeasures

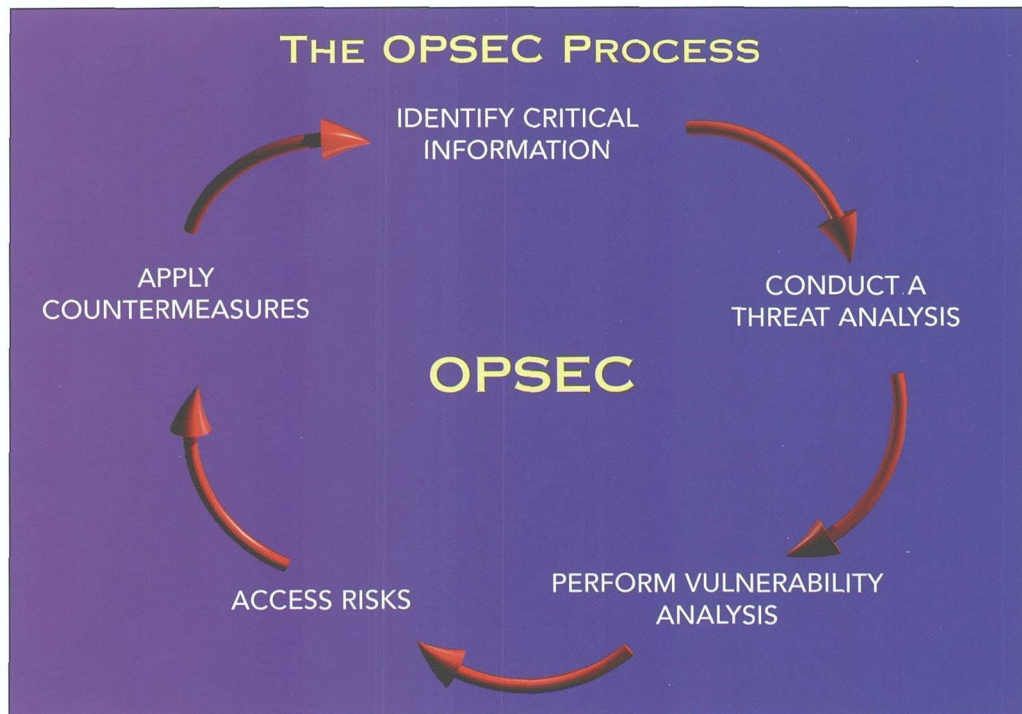


FIGURE 3-5 OPSEC is a fluid process.

The reason these five steps are not numbered is that the process does not have to be followed sequentially in a linear fashion. OPSEC is a fluid process that allows the Team Leader to use the system in a manner that fits the particular

situation. OPSEC can be used as part of a formal mission planning process or it can be implemented real time at a crime scene. In many respects, OPSEC is like the Incident Management System "toolbox." You select the right component and begin the process with the best tool for the job at the time you need it. See Figure 3-5.

What makes OPSEC different from other security management procedures is that OPSEC focuses directly on the threat.

INTERAGENCY OPERATIONS SECURITY SUPPORT STAFF



www.iooss.gov

In 1988, President Reagan signed National Security decision Directive 298, establishing the National Operations Security Program as a means to identify, control, and protect unclassified information and evidence associated with U.S. national security programs and activities. If not protected, such information often provides the opportunity for exploitation by adversaries or competitors working against the interests of the United States. The Directive names the Director, National Security Agency as the Executive Agent for Interagency OPSEC training and includes in his responsibilities the establishment of maintenance of the Interagency

OPSEC Support Staff. By mandate, this organization comprises representatives from the Federal Bureau of Investigation, Central Intelligence Agency, Department of Energy, General Services Administration, and Department of Defense including the National Security Agency. Other government organizations are not precluded from providing personnel to this staff and are encouraged to do so or to participate in interagency OPSEC forums.

The primary mission of the Interagency OPSEC Support Staff is to act as a consultant to other U.S. government departments and agencies, providing technical guidance and assistance that will result in self-sufficient OPSEC programs throughout government and the protection of U.S. operations. Members of this organization possess specialized technical skills and are available to conduct OPSEC surveys, assess OPSEC programs, or provide training in operations security and analytical risk management.

The Interagency OPSEC Support Staff supports the National OPSEC Program through multimedia products, tailored training, and the presentation of activities and events that attract attendees from the security, intelligence, research and development, acquisition, and law enforcement communities. These events include the National OPSEC Conference and Exhibition, National Threat Symposium, and Regional Training Symposia.

FIGURE 3-6

NOTES

IDENTIFYING CRITICAL INFORMATION

Protecting Critical Information is paramount to the success of our public safety mission because Critical Information in the hands of our adversaries assures our failure. But what is Critical Information and how do we identify it?

Protecting Critical Information means safeguarding any information that reveals the specific facts about our intentions, capabilities, and activities needed by our adversaries for them to effectively plan an operation against us or guarantee the failure of our operation against them. For example, if we were a law enforcement Special Operations Unit and we were planning to arrest a suspected terrorist in his home and execute a search warrant for explosives, our Critical Information might include:

- **Capabilities**—What are we capable of doing based on our equipment and training? What are our limitations?
- **Intentions**—What are we planning to do?
- **Place**—Where are we planning to do it?
- **Time**—When are planning to do it? Today, tomorrow, or next week?
- **Strength**—What personnel and other resources will we use?
- **Communications**—What radio frequencies will we operate on? How will we communicate with supporting agencies?
- **Tactics**—How will we execute the search warrant and arrest the suspect?
- **Vulnerabilities**—What and where are our weaknesses? Can the guy we are going to arrest take advantage of this?

Critical Information can be viewed from two perspectives: Ours and the Adversary's. From our perspective, we would consider information that we feel needs protection from our vantage point. There are a couple problems with using only our perspective:

- The Bad Guys might be targeting information that we failed to recognize that would be important to them.
- We might spend a lot of time and money protecting information that the Bad Guys already have.

If we only protect information that we feel is critical, the adversary might target information that is actually of greater importance to them. To illustrate this point for public safety, let's look at an example:

A light bulb manufacturer from a foreign country wanted to visit a light bulb factory of its competitor in England to discuss issues of mutual concern to the the light bulb industry. After several discussions on the telephone, the visit was approved by the company in England.

The factory in England knew that the light bulb filament they made was sensitive trade secret information, so they did not let the visitors from the other company view the manufacturing process of the light bulb filament. However, being very proud of their plant, they took the visitors on a tour of the light bulb assembly area. Months later, much to the surprise of the factory in England, the very same type of light bulb made by the company in England came on the market at a cheaper price. It was produced by the same foreign company that visited the plant earlier in the year. As it turns out, the foreign company already knew how the filament was made, what they did not know was how the company in England assembled the light bulb so efficiently. By touring the plant they were able to obtain the critical information they needed. The company in England protected the information that was critical to them, not the information that was critical through the eyes of their competitor.

As a public safety agency, we must look at our operations through the eyes of the Adversary. (Remember, there can be more than one adversary.) The question we need to ask ourselves is: What is it about our operations that we would not want an adversary to know?

Critical information consists of information and observable actions about our activities, intentions, capabilities, or limitations, which must be controlled to prevent an adversary from gaining a significant strategic or tactical advantage on us.

One misconception about the OPSEC process is that it is about protecting classified information, e.g., national security information such as Top Secret, Secret, and Confidential information protected under federal law. The fact is that practicing good OPSEC is primarily about protecting unclassified open source information that can easily be obtained by anyone who is skilled and motivated to simply read about and observe our day-to-day operations.

Most law enforcement and security professionals begin the OPSEC process by determining what type of Critical Information needs to be protected and kept from our adversaries. Exactly what type of information needs to be protected depends on how you are applying OPSEC and the type of operations being conducted. Here are three practical examples:

EXAMPLE #1—You are part of a team conducting an investigation of a Hate Group suspected of bombing churches in your community. The critical information that needs protection is that you are actually conducting an investigation of the suspected group. If the group knew they were suspects and were the focus of an investigation, the investigation might be compromised and the suspects would not be arrested.

EXAMPLE #2—You are the Team Leader of a Public Safety Task Force developing special counterterrorism plans for a national level event being held in your community next year. Your Critical Information would be the special plans and procedures being developed. If the adversaries knew what your plans for countermeasures were, they could defeat them.

NOTES

EXAMPLE #3—You are the Special Agent-In-Charge at a major crime scene where a car bomb has killed 14 people. You have adopted a strategy and goals for proceeding with the investigation. Your team has some physical evidence and a few leads. The critical information that you need to protect is the evidence and the nature of the leads you are pursuing.

Under ideal conditions, identifying the information that is critical to the safety and security of your operation should involve a formal and structured process. You should discuss, identify, and list the information that is critical to the success of your operation, then move onto the next step in the OPSEC process. As an expedient, this can be done in the field at the incident or crime scene. OPSEC simply gets integrated into the command and control process.

ANALYZING THE THREAT

Analyzing the Threat is the next step in the OPSEC process. It involves determining the capability of an adversary and his intentions to undertake any action detrimental to the success of your operations. Remember that an adversary is anyone who opposes, or acts against law enforcement and public safety's mission.

Analyzing the Threat consists of two separate elements. The first involves identifying which individuals or organizations pose a credible threat. The second element examines what the adversary's capabilities are to collect information against you. A credible threat is any adversary with both INTENT + CAPABILITY.

Examples of Intent include:

Motivation—The group or individuals must be motivated to commit the crime. For example, if the group has a specific doctrine, is there a corresponding event that might motivate the group to take violent action?

History and Behavior Pattern—Does the past history of the organization point to a commitment to violence? Has there been a change in behavior patterns that may indicate that the person has serious intent to commit a violent act; e.g., they have recently engaged in violent behavior?

Current Activity—Is there evidence that the group has been active and have group members been exhibiting suspicious behavior; e.g., buying guns, attending meetings as a group?

Examples of Capability include:

Technology—To what type of hardware and software does the group have access? Organized Crime, drug traffickers, and nation-sponsored terrorist organizations can be expected to have better technical capability than poorly financed groups, e.g., they may have access to military grade hardware.

Force Structure—How is the group organized and how many members do they have? Is the group a disciplined paramilitary organization with a command structure or is it poorly organized?

Mobility—What type of transportation resources does the group or individual have access, to support an operation? For example, does the group have access to an aircraft?

Geographic Access—Does the group have access to your location or the area you are protecting? For example, if the threat is based in Tokyo and the event you are protecting is in New York, how accessible and practical is it that members of the group will have access to the event?

THREAT ASSESSMENT

A Threat Assessment is a risk evaluation tool for analyzing a specific threat for a specific operation being planned or for a facility or installation being protected.

The current thinking in counterterrorism preparedness places a great deal of emphasis on evaluating the potential for what has been termed as an Asymmetric Threat. Asymmetric means that the threat places his strengths against your weaknesses rather than force-on-force attacks. The best recent example of an Asymmetric Threat was the terrorist attack on the USS Cole (2001) in Yeman where a garbage boat loaded with explosives was detonated next to the ship. See Figure 3-7.



US GOVERNMENT®

FIGURE 3-7 The USS Cole bombing is an example of an asymmetric threat.

NOTES

DEVELOPING A THREAT ASSESSMENT

The real key to developing an accurate Threat Assessment for your specific situation is by participating in joint-agency working groups and by maintaining regular liaison and routine coordination with local, state, and federal law enforcement and intelligence agencies. You must meet regularly to solidify critical partnerships that will pay big dividends in developing intelligence information.

Threat Assessments are based on Intelligence. There are two categories of intelligence: Unclassified and Classified.

Unclassified Threat Assessments—Are based on information that is gathered legally from Open Sources (described earlier in this chapter) or through Law Enforcement agencies using traditional police intelligence and investigative techniques. Professional OPSEC Consultants under contract to a law enforcement or public safety agency may also develop Threat Assessments.

The final work product of an Unclassified Threat Assessment is usually held in confidence and may be officially labeled as Law Enforcement Sensitive or For Official Use Only (FOUO) as protected under the Freedom of Information Act. Remember that FOIA only applies to federal agencies and FOUO information must meet specific criteria to be rated as Not Releasable. You should seek legal counsel.

Classified Threat Assessments—Classified Threat Assessments are rated as Top Secret, Secret, and Confidential. National Security laws and regulations strictly protect the information.

A Classified Threat Assessment can be conducted by any authorized federal agency using employees or contractors that have the appropriate security clearances and credentials. The final classified work product is treated as Classified National Security Information and is restricted to individuals who: a) Have the appropriate level of security clearance, and b) Have a need to know the information.

Not everyone can have access to classified information used to develop a Classified Threat Assessment. This is often the source of some friction between federal and local agencies that may be working in a Joint Operations format. But we need to appreciate that Information in Classified Threat Assessments is "classified" in order to protect intelligence sources and methods that were used to develop the Threat Assessment report. It is completely appropriate, and good OPSEC for a limited number of personnel within your group to have complete knowledge of the threat. It should also be obvious that until your organization shows that it has an OPSEC program in place, sensitive information simply is not going to be shared with you.

Any authorized federal law enforcement agency can use official channels to request assistance from another federal agency to help develop a Classified

Threat Assessment. However, you need to realize that the quality of the information that you get back is largely based on the level of detail you ask for. Vague requests will generate vague responses. The following federal agencies can support an authorized federal agency in providing threat assessment information.

- Central Intelligence Agency
 - Foreign Broadcast Information Service
- Defense Intelligence Agency
 - Armed Forces Medical Intelligence Center (AFMIC)
 - Central MASINT Organization
 - Combined Intelligence Publishing Service
 - Commonwealth Homepages (Australia, Canada, United Kingdom)
 - Defense Special Missile and Astronautics Center
 - Directorate for Intelligence
 - Directorate for Intelligence Operations
 - Directorate for Intelligence Production
 - Missile and Space Center
- Defense Threat Reduction Agency
- Department of Energy Office of Intelligence (DOE)
- Department of State Bureau of Intelligence and Research
- National Assurance Technology Center
- National Counterintelligence Center
- National Imagery and Mapping Agency (NIMA)
- National Reconnaissance Office (NRO)
- National Security Agency
- Nonproliferation Center
- U.S. Customs Service
- Federal Bureau of Investigation (FBI)
- U.S. Department of Commerce
- Defense Security Agency (DSS)
- Defense Technology Security Agency
- U.S. Bureau of Alcohol Tobacco and Firearms (BATF)
- Federal Aviation Administration

NOTES

- Federal Emergency Management Agency
- United States Secret Service (USSS)
- Defense Advanced Research Projects Agency (DARPA)
Counterintelligence Section
- Defense Information Systems

- U.S. Air Force
Directorate of Intelligence, Surveillance, and Reconnaissance
Air Force Office of Special Investigations
Air Intelligence Agency
- U.S. Army
Intelligence and Security Command (INSCOM)
Army Counterintelligence Center
National Ground Intelligence Center
- U.S. Navy
Naval Criminal Investigative Service (NCIS)

RATING THREATS

Ultimately, the final work product of analyzing the threat should incorporate a simple rating of whether the threat to your operations is High, Medium, or Low.

Professional OPSEC practitioners sometimes rate threats using a point system tied to specific definitions. To keep it simple, and for purposes of illustrating the process, we have rated threats as High, Medium, and Low.

High Threat—Means that an adversary has both the intent and capability and can collect the desired information against you more than 90% of the time.

Medium Threat—Means that an adversary has both the intent and capability and can collect the desired information against you more than 30 to 70% of the time.

Low Threat—Means that an adversary has both the intent and capability and can collect the desired information against you less than 10% of the time.

A simple Threat Assessment Model can be used to illustrate the relationship between a High or Low Threat based on Intent and Capability. Threats that we believe fall in the high range of INTENT + CAPABILITY should receive a more focused evaluation and go through a formal Threat Assessment process.

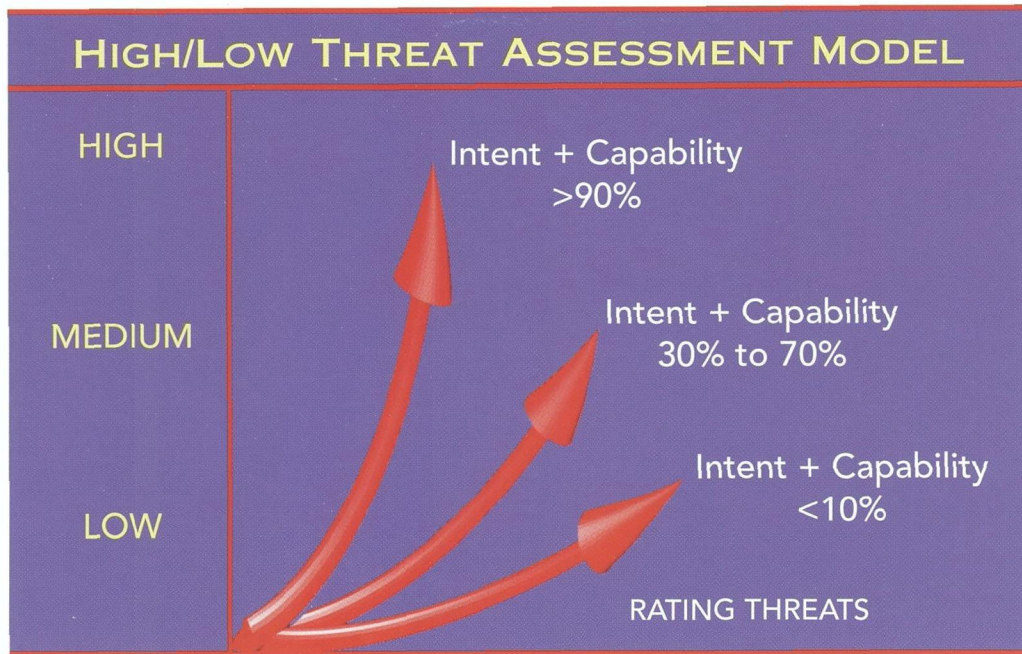


FIGURE 3-8

ANALYZING VULNERABILITIES

The next step in the OPSEC process is to evaluate the capability an adversary has to disrupt or stop your operation. This requires examination of your Vulnerabilities and Indicators.

Vulnerabilities—Are the weaknesses associated with the ways you protect your critical information or weaknesses that are subject to exploitation by an adversary.

Some examples of Vulnerabilities include:

- Units have no encrypted communications capability. All radio and cellular telephone transmissions are in the clear and are vulnerable to monitoring.
- Planning meetings for the team are held in public restaurants where informers may overhear operational details.
- Access to mission planning areas are poorly controlled. Many people have unrestricted access to office areas.
- There is no trash management plan in place for areas producing law enforcement sensitive information. Critical information is not shredded.
- Operational plans and timelines are circulated on unsecure e-mail accounts. Officers use home e-mail accounts to coordinate mission related activity.
- It is human nature to want to share stories about our job related-successes and failures with friends and family. Someone who is not security savvy can easily share some small bit of critical information with a friend, who inadvertently shares it with another person, and so on.

NOTES

- An honest person who has been manipulated or fooled by a third party to reveal information could be an unwitting participant and represent a vulnerability. Intelligence agents, hackers, and crackers, are experts at using elicitation and social engineering techniques to get information without revealing their actual intent. The participant often does not even realize that they have compromised sensitive information.

Indicators—Are there any observable or detectable activities that project a weakness in your organization or reveal information concerning an operation you are planning. For example, if the Police SWAT Team is donning tactical gear in the police station parking lot that could be a pretty strong indicator to drug dealers that a clandestine lab raid is going down.

Some examples of Indicators include:

- Types of undercover police cars used and the types of antennas used.
- Special Operations Team uniform patches that may signal a Special Operations team is assembling for an operation in an area.
- Changes in behavior patterns, e.g., the only time the HazMat Coordinator meets with the SWAT Team Commander is when there is a Meth Lab raid.
- The numbers, ranks, and types of personnel who attend a meeting on a particular day.
- Increased activity in a particular area.
- Use of encryption features on public safety and law enforcement radios when encryption is not normally used for routine operations. Be aware that the sudden use of secrecy can actually become an indicator that a special operation is going down.

ASSESSING THE RISK

The Risk Assessment phase of the OPSEC process involves determining the probability that an adversary will succeed in compromising your critical information and evaluating the impact that it would have on your operation.

Risk Assessment weighs three basic factors based on the information that has been developed in the OPSEC process. These include:

1. **Threat**—Do(es) the Adversary(s) have Intent and the Capability? What does the Threat Assessment that has been conducted tell you?
2. **Vulnerability**—What type of opportunity does the Adversary have to exploit the vulnerabilities that you have identified?
3. **Impact**—What would the impact on your operation be if the Adversary successfully took advantage of one of your vulnerabilities?

For field operations like protecting evidence at a crime scene, the OPSEC Risk Assessment process can consist of simple intuitive reasoning based on personal experience, local knowledge, and past history. For more complicated missions

like planning for national level events, a formal committee approach may be needed. The more threats and vulnerabilities identified, the more complicated the risk assessment process will need to be.

ANALYSIS CHART				
THREAT	VULNERABILITY	VUL	IMPACT	RISK
HI	Personnel's lack of threat awareness	HI	MHI	HI
MHI	Use of non-secure communications	MHI	HI	MHI
MED	Personal equipment	MED	MHI	MED

FIGURE 3-9

DEVELOPING AND APPLYING COUNTERMEASURES

Countermeasures are anything that effectively negates or reduces an adversary's ability to exploit our vulnerabilities. If the Risk Assessment step identifies that we have a vulnerability to compromising critical information and we are projecting indicators of our intentions, then we should consider some type of countermeasure.

Examples of Countermeasures include:

- Prohibiting discussion of the operation over the radio. Using encryption features would protect conversations, but if encryption is not used routinely, then implementing this countermeasure could actually become an Indicator to the Bad Guys that an operation is about to occur.
- Holding mission planning meetings at a neutral location that has a low risk of being watched by an adversary. Personnel can arrive at different times and entrances to reduce the risk of detection.
- Making face-to-face contact with key personnel to minimize risk of normal communications being compromised.
- Minimizing any change in work habits, schedules, or routines.
- Limiting the number of personnel who have access to the mission planning area.

The number and type of countermeasures that can be implemented depend on the time available, resources, and level of risk. Not every vulnerability and indicator needs to be fixed with a countermeasure. The Threat Assessment and Risk Assessment tools help guide your decision-making.

NOTES

OPSEC PRACTICAL EXERCISE

A State and Federal Law Enforcement Task Force has been closing in on an organized crime group that has been hijacking tractor-trailers of hazardous chemicals that are used as precursor chemicals for manufacturing illegal drugs. The group has been operating from a warehouse where trucks are unloaded and the chemicals are repackaged into smaller unmarked containers, then shipped and distributed to clandestine drug labs for processing. Months of careful surveillance and planning have gone into the operation. The Task Force plans to conduct a simultaneous take-down of ten labs and the warehouse in two weeks.

You are the Chief of Special Operations for the county fire department. At the request of the DEA, your fire department has been asked to support the Task Force during the take-down operations. You have specifically been asked to make the fire departments' mobile Command Post, the Hazardous Materials Response Team, the Bomb Squad, and HazMat Paramedics available to support the Task Force. In addition to hazardous materials concerns, the operators of the labs have been known to rig booby traps in the labs when they are not operating. The booby traps are usually rigged to create a major fire and explosion to destroy evidence.

For security reasons, you have not been given specific details about the name of the criminal group, the locations of the warehouse and labs, or the specific date and time of the take-down. You have met members of the task force but you do not know the last names of the participants or the agencies they work for. But, for planning your side of the operation, you have been given very detailed information on the types of hazardous materials that will be present as well as details on the types of improvised explosive devices that may be found.

Your first job is to develop an OPSEC plan that will ensure a safe and effective operation and will safeguard sensitive law enforcement information. See Figures 3-10 on pages 38 and 39 for examples of completed OPSEC Worksheets.

CHAPTER SUMMARY

Security needs to be incorporated into the public safety culture and it must become the routine for how we operate, not the exception.

Operations Security (OPSEC) is a risk management tool used to deny an adversary information concerning our intentions and capabilities by identifying, controlling, and protecting indicators associated with the planning and execution of law enforcement and public safety missions.

The OPSEC process consists of five different steps: 1) Identifying Critical Information; 2) Conducting a Threat Analysis; 3) Performing a Vulnerability Analysis; 4) Assessing Risks; and 5) Applying Countermeasures.

Operations Security (OPSEC) has proven its worth many times over to the military and law enforcement agencies. The benefit of retaining the element of surprise and protecting the integrity of the mission can have a significant impact on the safety and success of your operations in both the planning and operational phases.

REFERENCES

NOTES

Carus, Seth, W., BIOTERRORISM AND BIOCRIMES: THE ILLICIT USE OF BIOLOGICAL AGENTS IN THE 20TH CENTURY, CENTER FOR COUNTERPROLIFERATION RESEARCH, NATIONAL DEFENSE UNIVERSITY, (MARCH 1999).

George, John, and Wilcox, Laird, AMERICAN EXTREMISTS: Militias, Supremacists, Klansmen, Communists, & Others, Amherst, New York, Prometheus Books, (1996).

Glorioso, John, E. and Ritter, Robert, B., "Maintaining Operational Security: Minimizing the Risk of Law Enforcement Mission Failure", LAW AND ORDER, Vol 44, No. 10, (October 1996).

Hildebrand, Michael, S., and Glorioso, John, E., OPERATIONS SECURITY FOR SPECIAL OPERATIONS TEAMS, International Association of Fire Chiefs, Hazardous Materials Response Teams Conference, Towson, Maryland, (June 4, 2000).

Hildebrand, Michael, S, and Mauriello, Thomas, P., OPERATIONS SECURITY FOR FIRE DEPARTMENTS, International Association of Fire Chiefs, Best Practices, Great Leaders National Teleconference, Greenbelt, Maryland (June 3, 2000).

Nolan, John, CONFIDENTIAL: "Uncover Your Competitors' Top Business Secrets Legally and Quickly- and Protect Your Own", Harper (1999).

Power, Richard, TANGLED WEB: Tales of Digital Crime From the Shadows of Cyberspace, Que Corporation, (2000).

Smithson, Amy E. and Levy, Leslie-Anne, ATAXIA: THE CHEMICAL BIOLOGICAL THREAT AND THE U.S. RESPONSE, Report No. 35, The Henry L. Stimson Center, (October 2000).

U.S. Central Intelligence Agency, Director of Central Intelligence, George Tenet's remarks on, REPORT TO CONGRESS ON THREATS TO NATIONAL SECURITY (February 2001).

U.S. Central Intelligence Agency, GLOBAL TRENDS 2015: "A Dialogue About the Future With Nongovernment Experts", NOC 2000-02 (2000).

U.S. Commission on National Security/21st century, Road Map for National Security: Imperative for Change (January 2001).

U.S. Interagency OPSEC Support Staff, OPERATIONS SECURITY: Program Managers Handbook, (2000).

U.S. Interagency OPSEC Support Staff, GLOSSARY OF OPSEC TERMS, (1998).

U.S. Department of Justice, Federal Bureau of Investigation, THE SCHOOL SHOOTER: A THREAT ASSESSMENT PERSPECTIVE (2000).

U.S. Department of Justice, Federal Bureau of Investigation, PROJECT MEGIDDO (1999).

U.S. State Department, PATTERNS OF GLOBAL TERRORISM (October 1999).

U.S. State Department, FOREIGN TERRORISTS ORGANIZATIONS, (October 1999).

FIRE DEPARTMENT SPECIAL OPERATIONS OPSEC EXERCISE WORKSHEET

MISSION : Provide Fire/HazMat/EMS- Special Operations Support for Law Enforcement Task Force

Critical Information	Threat		Vulnerabilities		Risk	Countermeasures
	Adversaries	Collection Methods	Indirect (Indicators)	Direct (Source)		
Types & quantity of HazMat used as precursors chemicals.	<u>ACTIVE ADVERSARY</u> Organized Crime Drug Cartel (Well funded. Professional Intelligence Officers. Top quality hardware)	Close-in cell phone monitoring.	1. Using cell phones.	4. Request for authorized overtime for Special Operations at Council meeting live T.V. broadcast.	1. Medium 2. High	1. Communicate mission related info. in face-to-face meetings. Continue normal cell phone use, but do not discuss mission on cell phones.
Types of Improvised Explosive Devices the Meth Lab Operators use.	Clan Lab Operators (Receive intelligence locally and from Cartel intel cell) Possible inside involvement of trucking company involved in hijackings. (Possible organized crime connection.)	Paid informants. Close-in radio interception.	2. Increased meetings with Law Enforcement by Chief Officers. 3. Location and time of meetings.	5. Paid informers operating in county offices. 6. Paid informers at local bars used by fire-fighters.	3. High 4. Medium 5. High	2 & 3. CM= Change times and locations of meetings. Meet in buildings with underground garage. Arrive and depart at different times and entrances. 4. CM= Request Fire Chief not mention overtime request in open meeting. Do not reveal reason for overtime to administrative staff.

Critical Information	Threat		Vulnerabilities		Risk	Countermeasures
	Adversaries	Collection Methods	Indirect (Indicators) (Source)	Direct		
<p>Fact that the Fire Department is supporting the Task Force.</p> <p>Names of agencies involved.</p> <p>Fact that Task Force is focusing on 10 Meth Labs and a warehouse.</p> <p>Date and time of operation (once known to fire department.)</p>	<p><u>PASSIVE ADVERSARY</u></p> <p>Informers working in City Office Building.</p> <p>Restaurant and Bar patrons at places frequented by police and fire.</p> <p>Drug dealers on the street.</p>	<p>Paid informer running home server interception of e-mail.</p> <p>Dumpster Diving at County Office Buildings</p> <p>Paid informers working in city buildings.</p> <p>Informers (drugs for information).</p>	<p>4. Number of people involved in meetings.</p>		<p>6. High</p>	<p>5. & 6. Brief Special Operations personnel of the risk. Need to limit information, maintain routine. Avoid public disclosure.</p>

Personnel and Organizations Briefed on Elements of the Operations: 1. State Police Commander, 2. County Police Narcotics Division Commander, 3. DEA Special Agent in Charge, 4. States Attorney General Organized Crime Bureau Chief Investigator, 5. Bomb Squad Commander, 6. Chief of EMS, 7. HazMat Team Shift Commanders A&B. 8. Deputy Chief, Fire Department Special Operations Division.

Total personnel cleared into the operational planning of the mission with Need-To-Know all aspects of the operation = 9 Personnel
 Total number of personnel involved in Task Force in some phase of the operation = 85

FIGURE 3-10

Interagency OPSEC Support Staff

6411 Ivy Lane; Suite 400
Greenbelt, Maryland 20770-1405
IOSS: (301) 982-0323 FAX: (301) 982-2913
www.ioss.gov

HSERC
August 15, 2002
HMEP PLANNING GRANT
FY 03

The primary objective of the planning grants program is to develop, improve, and implement emergency plans under EPCRA.

Available funds:

Federal Funding:	\$43,006
State Funding:	<u>\$10,752</u>
Total	\$53,758

PROJECT PROPOSALS

Honolulu LEPC \$24,000 (Federal: \$19,000; State: \$4,800)

Scope: To conduct risk assessments for fixed facilities in the vicinity of Honolulu Harbor that store or utilize hazardous chemicals.

Maui LEPC \$9,500 (Federal: \$7,600; State: \$1,900)

Scope: To continue the Facility Profile Planning Process.

Hawaii County LEPC \$14,200 (Federal: \$11,360; State: \$2,840)

Scope: To continue and expand the study of geographical response patterns and response times for hazardous materials incidents in Hawaii County over the past eight years. To affirm the current distribution of resources and to recommend changes if deemed necessary.

Kauai LEPC \$6,058 (Federal: \$4,846; State: \$1,212)

Purchase computer hardware, software and materials for planning activities.



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
REGION IX
75 Hawthorne Street
San Francisco, CA 94105

EPA Update for Hawai'i SERC Meeting August 15, 2002

Security for Public Water Systems

In June, President Bush signed into law the Public Health Security and Bioterrorism Preparedness and Response Act. Public water systems serving a population greater than 3,300 are required to certify to the EPA that the system has completed or revised an Emergency Response Plan that incorporates the results of a vulnerability assessment.

Site Security for Chemical Facilities

EPA Headquarters is evaluating with OSHA, the Justice Department and others about determining whether the General Duty Clause of the Clean Air Act Amendments provides EPA the authority to conduct site security reviews for chemical facilities.

Vulnerability assessments are an integral part of site security and EPA has developed a training class based on Sandia National Laboratories' vulnerability assessment model. The class audience will be federal, state and local regulators in addition to industry. This model is aimed at large chemical facilities and businesses. EPA Region 9 will host a training class Nov. 12 - 14 in San Francisco. Classes will also be held in Kansas City on Sept. 24 - 26 and in Atlanta on Oct. 22 - 24. An overview of the vulnerability methodology will be given during the first day of the training. The remainder of the workshop will be focused on applying the methodology. The registration fee is \$350 and class sizes are limited. Final details will be announced shortly.

Meanwhile, other vulnerability assessment model classes are available -- developed by the Chemical Center for Process Safety (an affiliate of the American Chemistry Council). In contrast to the Sandia model, these classes are aimed at medium to small facilities. Classes will be held in Houston on Sept. 9 - 10, in Baltimore on Sept. 12 - 13, and in New Orleans on Sept. 23 - 24. Information at: www.americanchemical.com under "Products and Services".

New CEPPPO Director in Washington and new CEPP Team Leader in Region 9

Debra Dietrich is the U.S. EPA's new director for CEPPPO in Washington, replacing Jim Makris who retired last month.

Kay Lawrence is the new CEPP Team Leader in San Francisco, replacing Mary Wesling who has been the Acting Team Leader since Nate Lau's promotion in March. Kay has been an On Scene Coordinator in EPA Region 9 for nine years. Before her work in Region 9 she developed considerable inspection and enforcement experience in EPA Region 7.

Upcoming Conferences

- Continuing Challenge in Sacramento, CA on Sept. 3-6. Website: www.hazmat.org
 - HazMat Explo in Las Vegas on Dec. 2-6. Website: www.hazmatexplo.org
- (A two-hour overview session by EPA regarding chemical site security vulnerability

assessments is scheduled for HazMat Explo.)

New CAMEO (Computer Aided Management of Emergency Operations) Now Available

A new expanded, faster CAMEO system is now available. It can be downloaded from www.epa.gov/ceppo using the 'What's New Button'.

Recent EPA Publications of Interest

Publications are available at 'What's New' on the EPA Chemical Emergency Preparedness and Prevention website: <http://www.epa.gov/ceppo/> or the Information Hotline at 1-800-424-9346.

LEPCs and Deliberate Releases: Addressing Terrorist Activities in the Local Emergency Plan (August 2001). In recent years, the threat of incidents involving chemical and biological materials has increased. This fact sheet discusses how LEPCs can incorporate counter-terrorism issues when they review and update their local plans.

Chemical Accident Prevention: Site Security (February 2000). As a precaution during this heightened state of alertness, the U.S. EPA in coordination with the U.S. Department of Transportation (DOT) and the Federal Bureau of Investigation (FBI) suggests that those who manufacture, distribute, transport or store hazardous chemicals should be especially vigilant regarding the physical security of those chemicals. In addition to this EPA advisory, DOT, has produced a separate advisory for transporters, available by contacting DOT at (202) 366-6525. The FBI requests that you expeditiously report any threats or suspicious behavior to your local FBI field office.

Other Recent Publications of Interest.

Site Security Guidelines for the U.S. Chemical Industry, developed by a group of company security professionals and designed specifically for the chemical industry, can help companies build upon their existing security programs. The guidelines outline typical elements of a good security program and suggest security practices that managers can consider and tailor to their facilities particular circumstances. This includes information on employee and contractor security issues, risk assessment, prevention strategies, training, emergency response and crisis management, and physical and cyber security issues. This document is available from the American Chemical Council website: www.americanchemistry.com/

CEPP Program Contact for EPA Region 9 (Pacific Southwest Region)


For more information about U.S. EPA's Chemical Emergency Preparedness and Prevention program in Hawai'i, please contact Mike Ardito at (415) 972-3081 or by email at ardito.michael@epa.gov

EPCRA and RMP Call Center

1-800-424-9346 (M-F, 9-5 ET) or www.epa.gov/epaoswer/hotline,
e-mail: epacallcenter@bah.com

EPA's Regional Response Center


EPA's office in San Francisco is expected to have its new Regional Response Center built this fall and have it operable in early 2003.



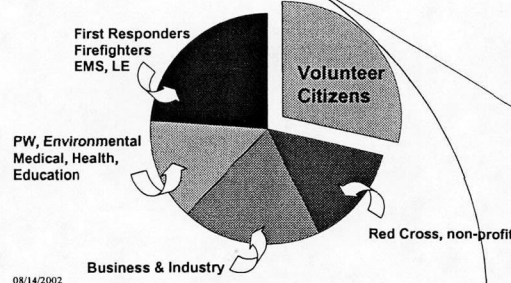
citizen★corps

Tessa Badua-Larsen
 FEMA Region IX
 510-627-7185 ph
 Teresita.badua-larsen@fema.gov


08/14/2002



SERC/LEPC




08/14/2002



USA Freedom Corps

- Peace Corps
- Corporation for National and Community Service (CNCS)
 - AmeriCorps
 - Senior Corps
- Citizen Corps


08/14/2002



citizen★corps

Citizen participation in Community Safety


08/14/2002



citizen★corps

- Opportunities for Citizen participation:
 - Emergency Preparedness
 - Mitigation practices
 - Crime prevention
 - Augment first responders


08/14/2002



citizen★corps

- Five Federal Programs:
 - Neighborhood Watch Program
 - Volunteers in Police Service (VIPS)
 - Community Emergency Response Teams (CERT) Program
 - Medical Reserve Corp
 - Operations TIPS


08/14/2002



citizen★corps

- Neighborhood Watch
 - DOJ
 - 30 years old
 - National Sheriff's Association
 - Expanded mission to incorporate terrorism prevention and education
 - Goal: 15,000 by 2004


08/14/2002



citizen★corps

- Volunteers in Police Service (VIPS)
 - DOJ
 - Launch - May 2002
 - International Association of Police Chiefs
 - Incorporate community volunteers
 - Administrative
 - Non-intervention
 - www.policevolunteers.org


08/14/2002



citizen★corps

- Community Emergency Response Teams
 - FEMA
 - Emergency Preparedness Training
 - Basic response techniques
 - Goal: 600,000 by 2004
 - www.FEMA.gov/EMT/CERT


08/14/2002



citizen★corps

- Medical Reserve Corps
 - HHS
 - Medical reserve volunteers
 - Support large-scale local emergencies
 - Promote local community public health
 - www.surgeongeneral.gov


08/14/2002



citizen★corps

- Operation TIPS
 - DOJ
 - Terrorism Information and Prevention System
 - Launch - Summer 2002 - 10 cities
 - Educational and training materials - industry


08/14/2002



citizen★corps

- ROLES:
 - Federal
 - State
 - Local


08/14/2002



FEDERAL ROLE

- Promote "Citizen Corps"
- Foster State and community participation
- Compile accurate information
- Set training standards
- Help identify volunteer programs and initiatives
- Help secure national partnerships
- Develop financial incentives and tie-ins


08/14/2002



State Role

- State Role:
 - Designate a Citizen Corps POC
 - Encourage every community to participate in Citizen Corps


08/14/2002



Local Role

- Citizen Corps Councils
 - Emergency Management
 - First Responders
 - Volunteer, community service, faith-based
 - Educational institutions, Medical facilities
 - Business & Industry
 - Community's neighborhood networks


08/14/2002



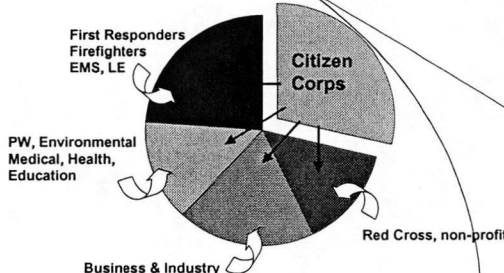
Citizen Corps Councils

- Objectives
 - Match skills
 - Educate
 - Spearhead volunteer opportunities
 - Promote Citizen Corps programs
 - Highlight accomplishments
 - Assess increased awareness


08/14/2002



SERC/LEPC



08/14/2002



citizen★corps


DOJ Grants

Supplemental -

FY03 - \$17m

- \$3m - NWP
- \$8m - TIPS
- \$6m - VIPS

08/14/2002



citizen★corps


HHS Grants

Supplemental - \$3m

- \$2m – Demonstration Projects
- \$1m – Tech Assist, contracts, website
- Application due: August 23, 2002

FY03 - \$10m

08/14/2002



citizen★corps


FEMA Grants

Supplemental -

- \$25m – Citizen Corp/CERT
- \$100m – Planning
- \$56m – EOC
- \$110 – Interoperable Communications
- \$7m – Secure communications

FY03 - ~~\$216m - \$156m - EOC~~

08/14/2002



Federal Emergency
Management Agency

citizen★corps

08/14/2002

Volunteer for Citizen Corps

Volunteer for America



Citizen Corps is a new network of volunteer organizations that utilize the skills and abilities of the American people to prepare communities for the threats of terrorism, crime and disasters. Citizen Corps is administered by the Federal Emergency Management Agency (FEMA) and is a vital part of the USA Freedom Corps, President Bush's initiative to encourage and assist all Americans to engage in service to their communities, our country, and the world.

At the local level, **Citizen Corps Councils** will help drive citizen participation within a community by coordinating Citizen Corps programs, identifying volunteer opportunities to support local law enforcement and emergency response personnel, and specifying local resources to support Citizen Corps. Citizen Corps programs include the following:

The **Community Emergency Response Team** program will train individuals in emergency preparedness and basic response techniques and enable them to prepare volunteers to take a more active role in providing critical support to first responders during emergencies.

An expanded **Neighborhood Watch Program** will incorporate terrorism prevention and education into its existing crime prevention mission and will expand the number of communities served.

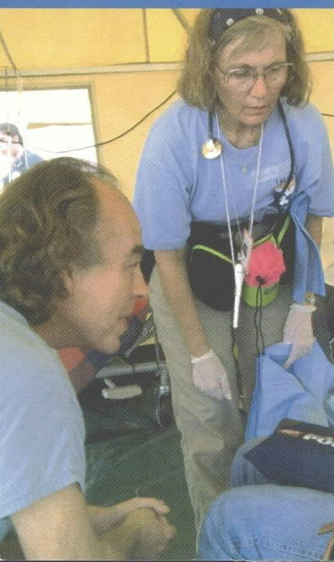
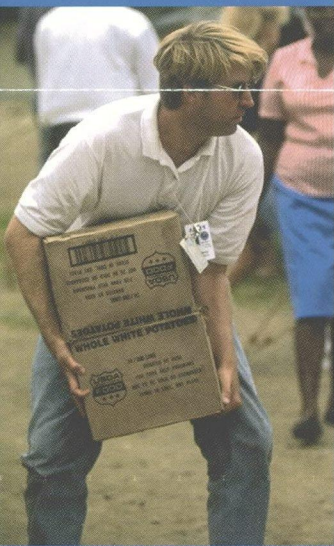
Volunteers in Police Service will provide support for resource-constrained police departments by tapping civilian volunteers to supplement their community's law enforcement professionals in order to free up sworn officers for frontline duty.

The **Medical Reserve Corps** will coordinate volunteer health professionals during large-scale emergencies to assist emergency response teams, provide care to victims with less serious injuries, and remove other burdens that inhibit the effectiveness of physicians and nurses in a major crisis.

Operation TIPS, the Terrorist Information and Prevention System, will be a nationwide program utilizing millions of workers who, by the nature of their jobs, are well-positioned to recognize unusual events. Operation TIPS will provide them with training, materials and a formalized way to report suspicious activity to the nearest FBI field office.

President Bush encourages all Americans to volunteer. You can also receive *The Citizens' Preparedness Guidebook*, created by the National Crime Prevention Council, featuring tips on preparing for the possibility of terrorism, crime and disaster. **Get the guidebook today by calling 1-800-WE-PREVENT (1-800-937-7383).**

**Volunteer your skills for America.
Sign up today for Citizen Corps!**



Visit our Web site at
www.citizen corps.gov



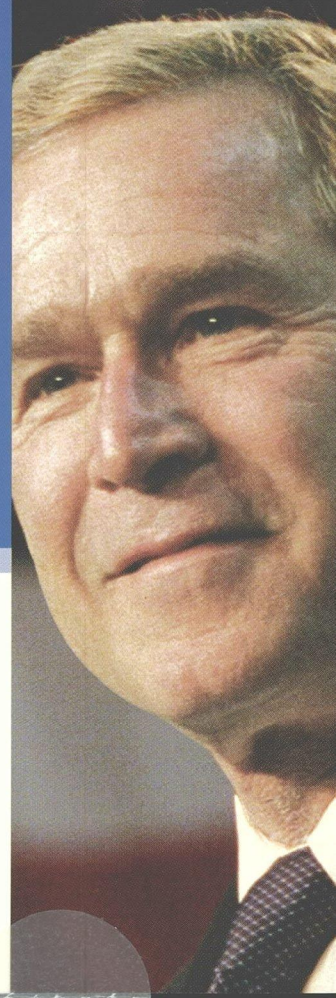
Volunteer at www.citizencorps.gov

“We want to be a nation that serves goals larger than self. We have been offered a unique opportunity, and we must not let this moment pass.”

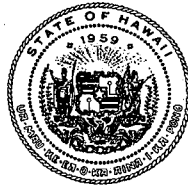
—President George W. Bush
State of the Union Address, January 29, 2002

citizen  ***corps***

Learn more about Citizen Corps and volunteer today!



BENJAMIN J. CAYETANO
GOVERNOR OF HAWAII



BRUCE S. ANDERSON, Ph.D.
DIRECTOR OF HEALTH

STATE OF HAWAII
DEPARTMENT OF HEALTH

In reply, please refer to:
HEER OFFICE

P.O. BOX 3378
HONOLULU, HAWAII 96801

HAWAII STATE EMERGENCY RESPONSE COMMISSION
MEETING #45

Thursday, January 10, 2002 from 9:07 a.m. to 10:50 a.m.

Department of Health
919 Ala Moana Boulevard, 5th Floor
Honolulu, Hawaii 96814

Final Meeting Summary

Attendees

Voting

Carter Davis, Oahu LEPC Representative
Gary Gill, Department of Health
Clifford Ikeda, Kauai LEPC Representative
W. Mason Young, Department of Land and Natural Resources
Glen Lockwood, American Red Cross
Joseph Blackburn, Maui LEPC Representative
Masayoshi Ogata, Department of Labor and Industrial Relations
Clem Jung, Department of Defense, Civil Defense Division
Robert A. Boesch, Department of Agriculture

Non-Voting

Jennifer Shishido, Department of Labor and Industrial Relations
James Decker, Department of Labor and Industrial Relations
Mike Cripps, Department of Health, Hazard Evaluation and Emergency Response Office
Curtis Martin, Department of Health, Hazard Evaluation and Emergency Response Office
Liz Galvez, Department of Health, Hazard Evaluation and Emergency Response Office
Denis Shimamoto, Department of Health, Hazard Evaluation and Emergency Response Office
Terry Corpus, Department of Health, Hazard Evaluation and Emergency Response Office
Joan Chang, Department of Health, Epidemiology Branch
Kathy Ho, Deputy Attorney General, State of Hawaii
Leland Nakai, Oahu Civil Defense
ENS Latarsha McQueen, Coast Guard
Marie Burd, Coast Guard
Jim Vinton, Tesoro Hawaii
Shirley Zhai, BEI Hawaii
Ron Ho, Department of Health, Clean Air Branch

Cynthia Pang, CNR HI

Keith Kawaoka, Department of Health, Hazard Evaluation and Emergency Response Office

Alan Sugihara, Navy Region Hawaii

Dennis Poma, BEI Hawaii

Beryl Ekimoto, Department of Health, Hazard Evaluation and Emergency Response Office

1) The meeting was convened at 9:07 a.m. by Gary Gill.

1.1 Attendees introduced themselves.

1.2 Minutes from meeting #44 were adopted with no changes.

1.3 Letter regarding coordinated purchases was sent to the mayors of each county.

2) LEPC Updates

2.1 Hawaii - No representative

2.2 Kauai

Clifford Ikeda - 1) A sewer spill occurred when a pump malfunctioned at a sewer plant and beaches were closed due to high bacteria count 2) Held a Kauai LEPC meeting in December 2001.

2.3 Maui

Joe Blackburn - 1) Sent two representatives to the December 2001 CEPP conference in Baltimore, MD to learn the new CAMEO, TIER II Submit. 2) Will be sending two representatives to the April 2002 NASTTPO conference.

2.4 Honolulu

Carter Davis – Gave an update of the January 7, 2002 Honolulu LEPC meeting as follows: 1) Gave an update of the status of the Honolulu City and County Emergency Operating Plan involving ammonia and chlorine 2) Leland Nakai and Carter Davis attended the HAZMAT Explo in Las Vegas, Nevada 3) FEMA is developing an internet HAZWOPPER training program 4) the mass casualty CHER-CAP sponsored exercise will be in May 2002 in Campbell Industrial Park 5) Update from CLEAN 6) Bruce Hisanaga, DOE, gave an update on “shelter-in-place” at seven schools around the Campbell Industrial area 7) BEI gave a presentation of a chlorine release that occurred on the Island of Lanai.

3) NASTTPO 2002 Update

Clem Jung - Gave an update of the annual NASTTPO conference that will be held from April 8-13, 2002 at the Ala Moana Hotel.

4) Explosives

Jennifer Shishido - Gave an update of the “explosives” issue. The inventory of explosives will be handled by PSD. Wording of the law was distributed, but the final version is still being drafted.

(Jennifer Shishido spoke earlier due to another scheduled meeting)

5) Chlorine Release

Dennis Poma made a presentation of a chlorine cylinder release that occurred at the Manele Wastewater Reclamation Facility on the island of Lanai. BEI will be donating related equipment to the counties to handle future chlorine releases.

6) EPA Update

Denis Shimamoto - handouts on EPA updates had been submitted by Mike Ardito and were available at the sign-in desk.

7) Access to Public Offices

Tom Smythe could not make the meeting. Defer to next meeting.

8) Other Business

ENS McQueen – Will be having an “Anthrax Focus Group” meeting at the Federal building on January 23, 2002 in room 209. Will be making an “anthrax appendix” and would like to have community input which will include roles, responsibilities, phone numbers, etc.

Jim Vinton – CLEAN donated \$31,000 for an improved communication system for Barbers Pt. School. The next CLEAN Board meeting will be on January 11, 2002.

Carter Davis – the City and County of Honolulu will have a display of various equipment for hazardous response at the next LEPC meeting.

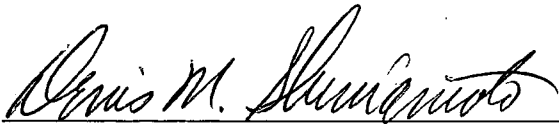
Masayoshi Ogata – The HIOSH website is online.

9) Schedule next HSERC meeting

The next HSERC meeting will be on Thursday, May 23, 2002 at 9:00 am.

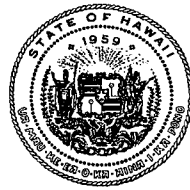
The meeting was adjourned at 10:50 am.

Respectfully Submitted



Denis M. Shimamoto, HSERC Coordinator

BENJAMIN J. CAYETANO
GOVERNOR OF HAWAII



BRUCE S. ANDERSON, Ph.D.
DIRECTOR OF HEALTH

STATE OF HAWAII
DEPARTMENT OF HEALTH

In reply, please refer to:
HEER OFFICE

P.O. BOX 3378
HONOLULU, HAWAII 96801

HAWAII STATE EMERGENCY RESPONSE COMMISSION
MEETING #46

Thursday, May 23, 2002 from 9:12 a.m. to 11:44 a.m.

Department of Health
919 Ala Moana Boulevard, 5th Floor
Honolulu, Hawaii 96814

Draft Meeting Summary

Attendees

Voting

Carter Davis, Oahu LEPC Representative
Gary Gill, Department of Health
Clifford Ikeda, Kauai LEPC Representative
Gary Moniz, Department of Land and Natural Resources
Joseph Blackburn, Maui LEPC Representative
Chris Takeno, Department of Transportation
Ed Teixeira, Department of Defense, Civil Defense Division
Robert A. Boesch, Department of Agriculture
Genevieve Salmonson, Environmental Quality Control Office
John Bowen, Hawaii LEPC Representative

Non-Voting

Mike Cripps, Department of Health, Hazard Evaluation and Emergency Response Office
Curtis Martin, Department of Health, Hazard Evaluation and Emergency Response Office
Liz Galvez, Department of Health, Hazard Evaluation and Emergency Response Office
Denis Shimamoto, Department of Health, Hazard Evaluation and Emergency Response Office
Terry Corpus, Department of Health, Hazard Evaluation and Emergency Response Office
Joan Chang, Department of Health, Epidemiology Branch
Leland Nakai, Oahu Civil Defense
Jim Vinton, Tesoro Hawaii
Todd Smith, FEMA Region IX
Mike Ardito, EPA Region IX
Terry Seelig, HFD
Clem Jung, SCD
Toby Clairmont, HAH

Cynthia Pang, CNR HI

Keith Kawaoka, Department of Health, Hazard Evaluation and Emergency Response Office

Alan Sugihara, Navy Region Hawaii

Beryl Ekimoto, Department of Health, Hazard Evaluation and Emergency Response Office

1) The meeting was convened at 9:12 a.m. by Gary Gill.

1.1 Attendees introduced themselves.

1.2 Minutes from meeting #45 were adopted with no changes.

2) Healthcare Association of Hawaii

Toby Clairmont, Healthcare Association of Hawaii, Emergency Program Manager, gave an overview of the Healthcare Association of Hawaii. (Presentation may be found at <http://www.HAH-Emergency.net/PUBLIC-library/HAH%20EMER%20Mgt%20Program%20Orientation.ppt>)

3) LEPC Updates

3.1 Hawaii

John Bowen – 1) MOA for the HMEP grant has been finalized and the HMEP project is ongoing; 2) Have several training programs for fire and police personnel; fire and police dispatchers; and EMS and News Media communication.

3.2 Kauai

Clifford Ikeda - 1) Federal Forestry conducted a three day ICS class with the utility facilities-hospitals, water, electricity; 2) sent participants to a WMD course; 3) Will be conducting a tabletop exercise August 13-14, 2002 with CST, SCD, and Kauai County; 4) There will be a Kauai LEPC meeting on June 19, 2002; 5) There will be a planning course for Fire, Police and EMS; 6) Will not be using all the HMEP Planning Grant Funds that were allocated to the Kauai LEPC because of the availability of other sources of funding.

3.3 Maui

Joe Blackburn - 1) Sent representatives to the April 2002 NASTTPO conference; 2) Purchased all the required equipment for MFD; 3) Trained personnel for the TIER II/Cameo data; 4) Will be retiring and intend to work for Maui Electric; 5) Would like to continue as the Maui LEPC Chair.

3.4 Honolulu

Carter Davis – Gave an update of the May 13, 2002 Honolulu LEPC meeting. (minutes enclosed)

4) NASTTPO 2002 Conference and 2002 Hazmat Training Calendar

Clem Jung – 1) Gave an update of the annual NASTTPO conference that was held from April 8-13, 2002 at the Ala Moana Hotel; 2) Distributed the 2002 Hazmat Training Calendar; 3) Possible field exercise in FY 04 for Hawaii County; 4) Possible field exercise in FY 05 for Kauai County; 5) Operation Kalaeloa exercise went well.

5) LEPC Funding

Curtis Martin – Presented the FY 03 HSERC Budget (see memo dated April 18, 2002). Motion to accept the budget was made and second. Unanimously approved.

Carter moved to have the LEPC operating funds of \$37,022 be distributed in the same way as last year but using the new percentages arrived at by the 2000 TIER II collection. Joe second. 8 approved, 1 abstain. The distribution will be as follows:

Honolulu	$\$5,000 + .444(\$17,022) = \$5,000 + \$7,558 = \$12,558$
Hawaii	$\$5,000 + .259(\$17,022) = \$5,000 + \$4,409 = \$ 9,409$
Maui	$\$5,000 + .175(\$17,022) = \$5,000 + \$2,979 = \$ 7,979$
Kauai	$\$5,000 + .122(\$17,022) = \$5,000 + \$2,076 = \$ 7,076$

6) EPA Update

Mike Ardito- EPA updates (see handout)

7) TIER II Submit as the Statewide System for Electronic Submission

Joe Blackburn – Will there be electronic submission of TIER II data by businesses? Maui County personnel are spending a lot of time in-putting TIER II data.

The DOH-HEER Office will be working on a format for a single electronic statewide data system for TIER II reporting so all the LEPCs will have access to the information.

Gary Gill stated that he would like to have Marsha Graf on the agenda for the next meeting to give the status of the electronic TIER II report data system.

8) Other Business

Jim Vinton-CERT (Community Emergency Response Team) CLEAN would like to focus on CERT training. Gary Gill stated to have Toby Clairmont at the next meeting to talk about CERT because Toby is the State representative.

Ken Chin stated that Tessa Badua-Larson will be the lead on this program. It will be called Citizen Core and it will include CERT, Neighborhood Watch and Americore. He will speak to Tessa on possible making a presentation at our next meeting.

Todd Smith- 1) Update on CHER-CAP exercises; 2) Hazmat Video Library will be transferred to the California Emergency Agency and videos will be available through them; 3) FEMA is being reorganized; 4) Office is moving to Oakland, CA; 5) \$900M for Fire Dept. grant will be available next fiscal year for basic needs and training.

9) Schedule next HSERC meeting

The next HSERC meeting will be on Thursday, August 15, 2002 at 9:00 am.

The meeting was adjourned at 11:44 am.



Emergency Management Program

**Toby L. Clairmont, RN, CEM
Emergency Program Manager
Healthcare Association of Hawaii**

**Assistant Hospital Administrator
Kaiser Foundation Hospitals - Hawaii**

Agenda...

1. **Mission of the Healthcare Association of Hawaii**
2. **Functions and components of
Emergency Management Program**
3. **Emergency response paradigms**
4. **Readiness development plan**

Mission Statement

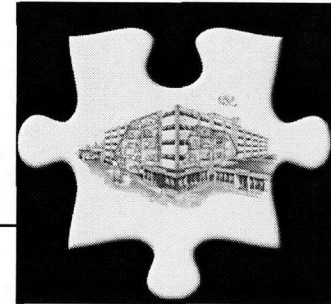
FOSTER mutual support among HAH member organizations through combined emergency preparedness planning, training and exercise activities

DEVELOP & MAINTAIN a forum for the exchange of information and technical support on emergency management issues affecting health care organizations

INTEGRATE & COORDINATE the actions of health care organizations in time of emergency with the intent of establishing and maintaining an effective and timely system-level response

ESTABLISH working partnerships with governmental and non-governmental emergency management organizations in the State of Hawaii

Whom we serve...



- 26 acute care Hospitals – 100%

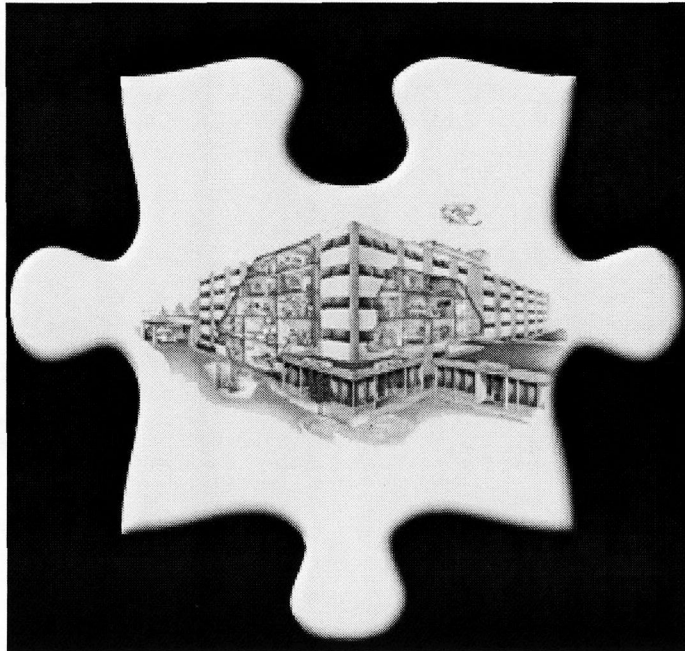
13	City & County of Honolulu
3	County of Kauai
4	County of Maui
6	County of Hawaii

- Specialty hospitals and Clinics
- Long Term care facilities
- Home Care agencies – *new in 2001*
- Hospice programs – *new on 2001*

... and whom depend upon as partners.

- **Civil Defense, Fire and EMS agencies**
- **State Department of Health**
- **American Medical Response**
- **Hawaii Air Ambulance**
- **Blood Bank of Hawaii**
- **Hawaii Nurses Association**

Hawaii hospitals today...



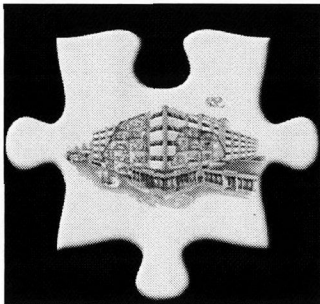
They typically have:

- JCAHO-compliant Emergency Management Plans
- Hazard Vulnerability Analysis- based planning processes

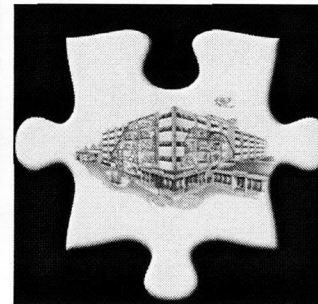
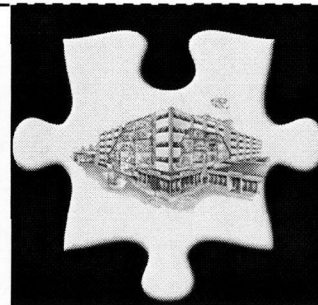
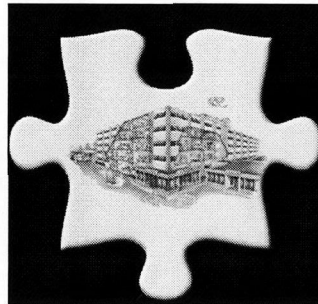
However they are also:

- Are geographically remote
- Have limited financial resources
- Have few unconstrained clinical resources – beds, staff

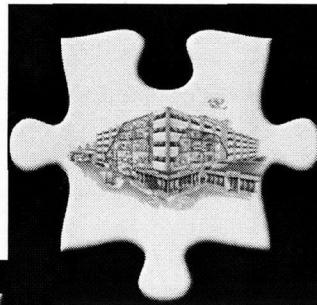
...function largely independently...



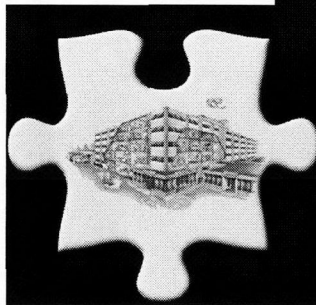
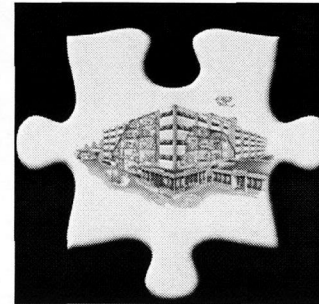
Health System A



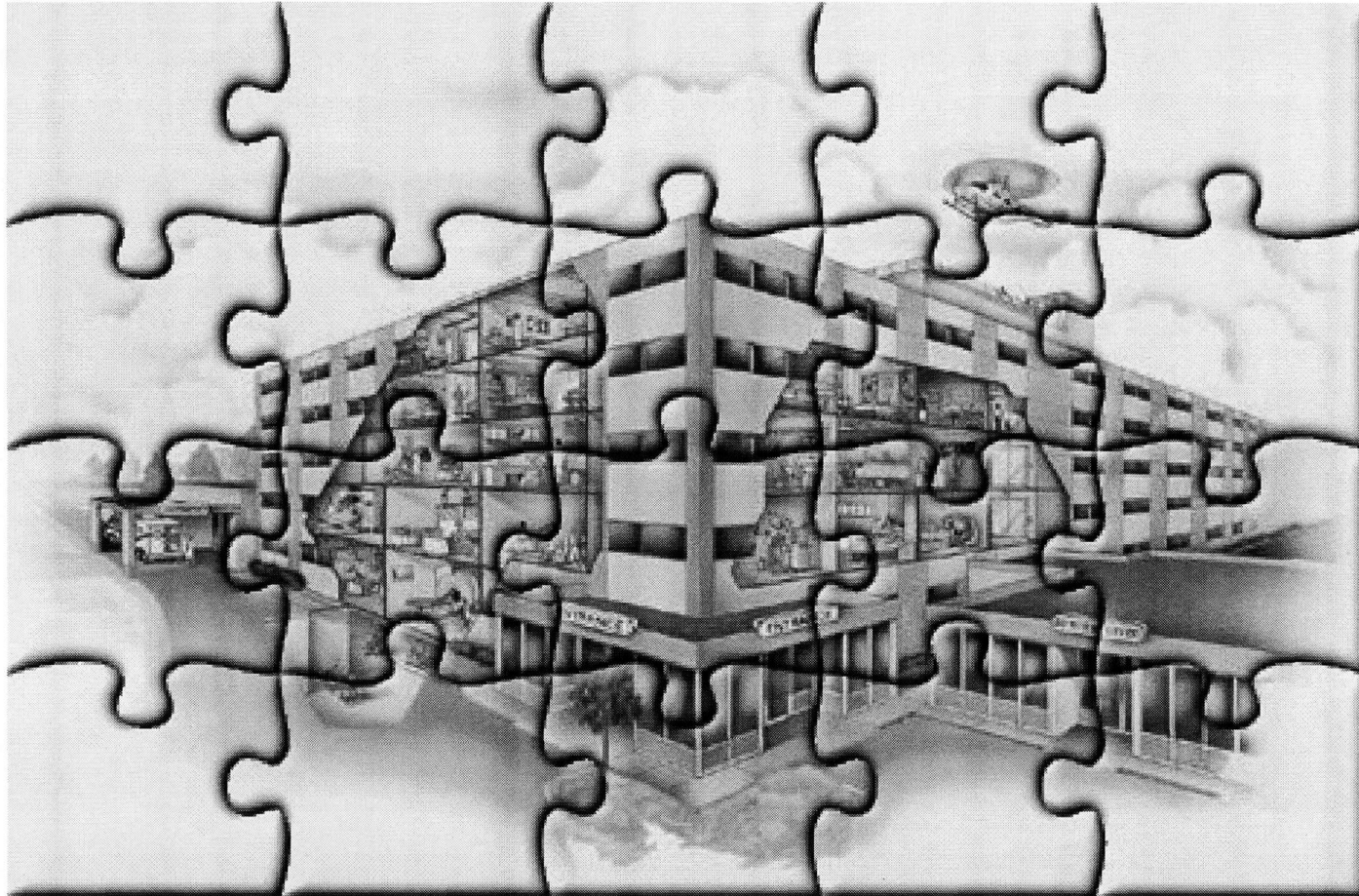
Health System B



Independent



...can also behave as an integrated hospital system during emergencies.



Emergency Management

**Program
Components**

Five program components...

1. Emergency Management Committee - governance
2. Emergency Program Manager - strategic leadership
3. Hospital Services Coordinating Plan - process
4. Health Care Organization Emergency Coordinators - tactical leadership
5. Strategic Partnerships - alignment

Emergency Management

Functions

12 defined management functions...

- **Leadership and Governance**
- **Hazard Identification, analysis & control**
- **Planning and Plans**
- **Direction, control and coordination**
- **Communications and warning**
- **Operations and procedures**
- **Resource management**
- **Logistics and facilities**
- **Public information**
- **Orientation and training**
- **Exercises**
- **Performance improvement**

Concept of Operations

Response Paradigms

Trauma Paradigm



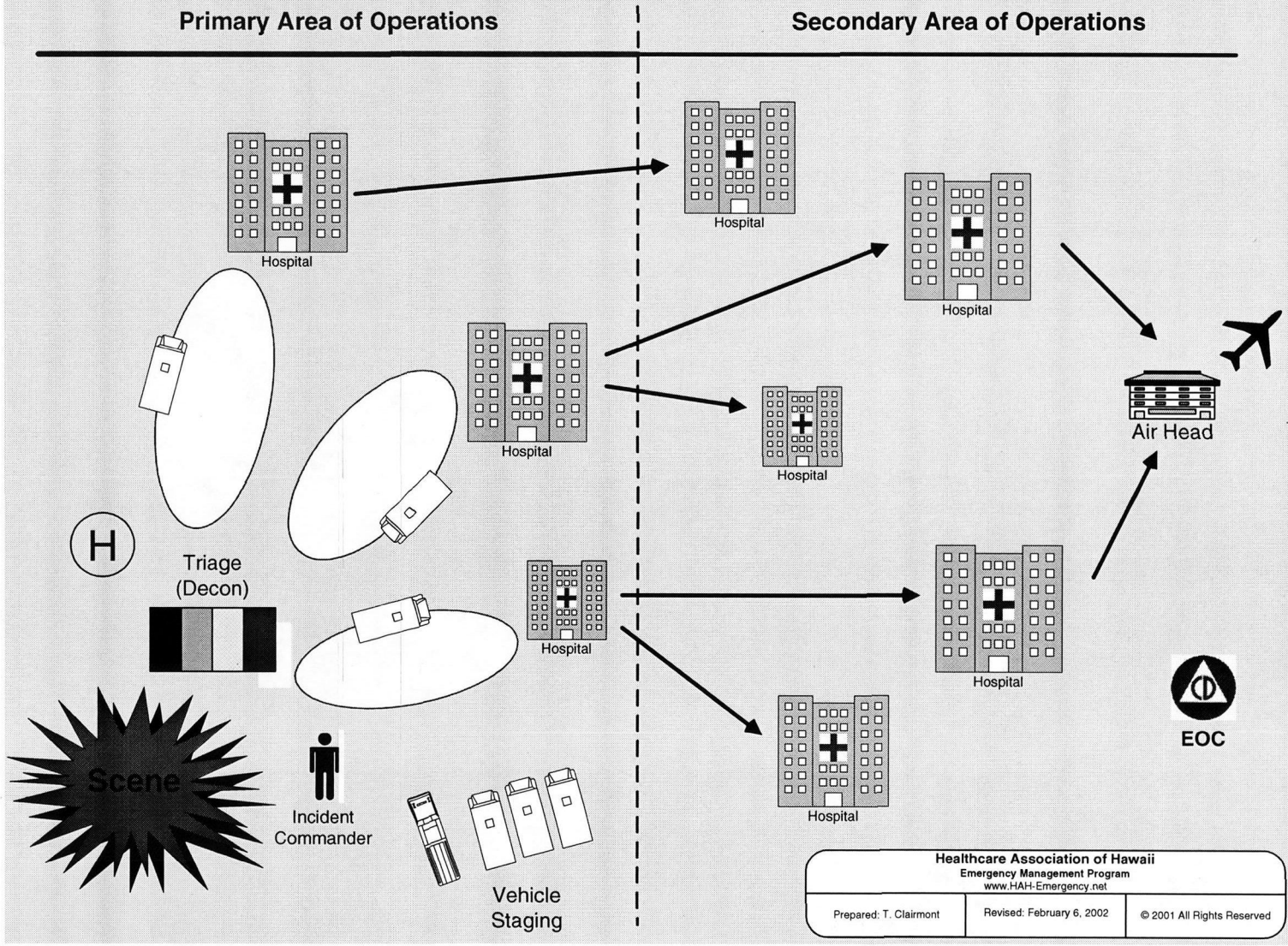
'GROUND ZERO'

- Focal (overt) event
- First responders are public safety agencies – EMS, fire, law enforcement
- Considerable experience, well understood
- Also used for acts of terrorism involving IED, chemical and nuclear devices

CONCEPT of OPERATIONS - TRAUMA EVENT

Primary Area of Operations

Secondary Area of Operations



Healthcare Association of Hawaii
 Emergency Management Program
 www.HAH-Emergency.net

Prepared: T. Clairmont Revised: February 6, 2002 © 2001 All Rights Reserved

Biological Paradigm



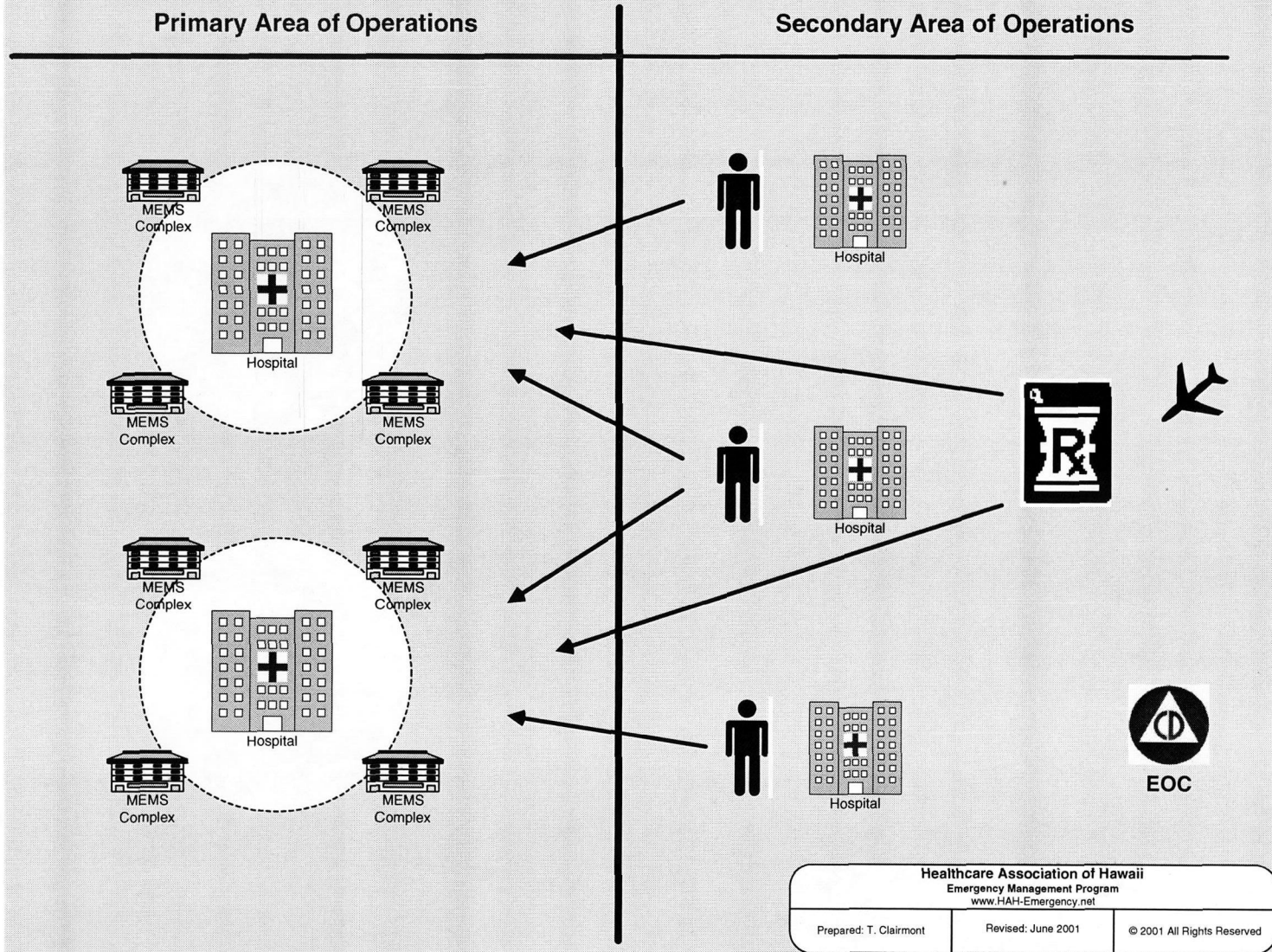
'GROUND ZERO'

- Multi-focal (covert) events
- First responders are primary care physicians and Emergency Departments
- No recent experience
- Also used for pandemic influenza

CONCEPT of OPERATIONS - BIOLOGICAL EVENT

Primary Area of Operations

Secondary Area of Operations



Healthcare Association of Hawaii
 Emergency Management Program
 www.HAH-Emergency.net

Prepared: T. Clairmont	Revised: June 2001	© 2001 All Rights Reserved
------------------------	--------------------	----------------------------



Healthcare Association
of Hawaii

Readiness Development 2002-2003

Funding...

- Congress approved \$1.1 billion for 2002-2003 period
- Department of Defense Appropriations Act of 2002 and Social Services Emergency Fund - 42 USC 247d
- Funding is available in three funding streams. Hawaii will receive a total of \$8,416,564

USPHS OEP for MMRS (Honolulu)	\$0.00
CDC for State DOH	\$7,697,208 (90%)
HRSA for hospitals	\$719,356 (10%)

- Funds for hospitals is administered by Health Resources and Services Administration (HRSA) via State DOH

HRSA first priority...

I. Medications and Vaccines

- On-site for emergency response up to 72 hours
- NPS for periods thereafter

II. Personal Protection & Decon

- Level C ^{plus}
- All facilities with an Emergency Department

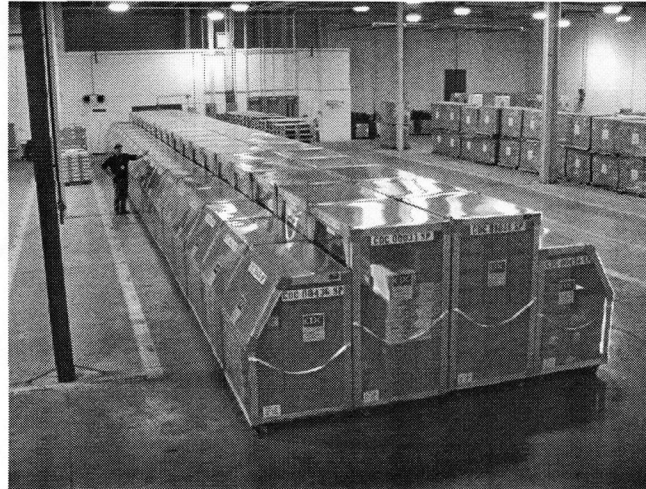
III. Communications

- Secure data and voice in all facilities

IV. Biological Disaster Drills

- Progress from tabletops to full scale exercises

National Pharmaceutical Stockpile



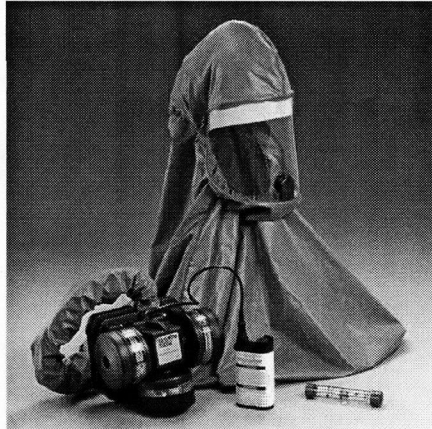
“to maintain a *national repository* of life-saving pharmaceuticals and medical materiel that will be delivered to the site of a chemical or biological terrorism event in order to reduce morbidity and mortality in civilian populations.”

Basic WMD Ensemble



- Uniform, decentralized
- MMRS compatible
- External, Modular decon

Includes Personal Protective Equipment



- Achieve level “C plus”
- HEPA equipped Respirator
- Protective over garment
- Gloves, boots...

HRSA second priority...

I. Personnel

- Planned use of ambulatory (outpatient) facilities
- Personnel to staff them

II. Training

- Leadership (planners, administrators)
- Functional (knowledge & skills for incident response)
- Tools for Awareness level in all organizations

III. Patient transfer

- Include ground and air ambulance
- NDMS



Action Plan...

Beginning IMMEDIATELY:

- Enhance HAH Emergency Management Committee
- Prepare & execute participation agreements
- Conduct detailed assessment using HCAR (version 2.00)
- Begin closing high vulnerability gaps
- Begin revision of HSCP and Hospital-level plans
- Provide leadership training



Then we'll...

- Explore use of ambulatory facilities
- Enhance data communications
- Plan to provide functional training
- Identify major equipment, supplies and pharmaceuticals needed to support 500 casualties
- Initiate long-range planning for a series of biological exercises (simulations)
- Review options to augment staffing



May 23, 2007
HSERC #46

①

9:12 am meeting convened by Jay Gill.
Minutes - mtg #45 approved.

Healthcare Facilities Overview.

- Toby Clarrmont - Healthcare overview Assoc of Hawaii ~~overview~~,
Emergency Program Manager.
- Sacred Falls - Trauma concept of operations
- 9/11 WTC

LEPC Updates

- John Bowen - MOA finalized HMAEP project ongoing
- Doing several training programs w Police, Fire
- Police, Fire dispatchers.
- ERAS & News media communication

Clifford Federal Forestry taught

- 3 days - ICS class ~~for~~ with utilities group - Hospitals,
Water, electricity
- WMAO course - sent participants to this course
- CST, SCD, Kawaii County - table top exercise
Aug 13-14
- June 19 LEPC mtg.
- Fire, Police, ERAS - planning course
- HMAEP funds - may not use this year's monies
due to other funds availability.
Cannot reconstitute too late in F.Y.

46 8 07 15

5/23/02
#46

(2)

Joe - purchased all equipment for MFD.

- Sent to MASTPO Conf.

- Prep. personnel for TIER II / CAMEO DATA

- Will be returning will work w/ Maui Electric.
Would like to continue as CEPC chair.

Carter - overview of 5/13/02 CEPC mtg.
Minutes attached

Chen Jung - April 8-13, 2002
MASTPO 2002 Conference overview.

- 2002 Hazard Training Calendar distributed.

Possible Field Exercise in FY04 for Hawaii County

" " " " FY05 " Kauai County

- Operation Kalaeloa exercise went well

CEPC Funding - Curtis Martin.

Motion - accept Budget 4/18/02 for FY03

HSEPC accept Budget,

Carter - Motion to distribute by CEPC

Joe Second

Motion withdrawn

Carter - motion funds distributed as last year

Joe second.

8 approved, 1 abstain.

EPA Update - Mike Audito - see distribution of update.

5/23/02
#46

3

TIER II Submit - Joe Blackburn

Electronic submission of TIER II data by business
DOH - HSEER office will be work out format
Single electronic statewide data system for
TIER II reporting so all CCEPC will
have access to information.

★ Next Agenda - Marsha - status of electronic
data ^{system} (TIER II report)

Other business

Joni Vinton - ~~SEPC~~ CCEPC

★ CCEPC to focus on ~~SEPC~~ training.
for as future agenda item - Toby Clammant.

Ken Chin - Tessa - Badua will be lead.

Citizen Core - ~~SEPC~~ CCEPC, Neighborhood Watch
America

Todd Smith - update of Chem-Cap exercise

- HAZMAT VIDEO Library will be
transferred to CCEPC California Emergency
Agency.

- FEMA reorganization

- Office moving to Oakland, CA

- Evon fire Dept available next fiscal year.
Basic needs & training

Next Meeting Aug 15, 2002

Meeting adjourned 11:44am.

Community
Emergency
Response
Team

**HONOLULU LOCAL EMERGENCY PLANNING COMMITTEE MEETING
MONDAY, MAY 13, 2002
HUMAN RESOURCES CONFERENCE ROOM**

The meeting was called to order at 9:07 A.M. by Chair Carter Davis.

I. INTRODUCTION/REMARKS/ADOPTION OF MINUTES

C. Davis welcomed everyone, gave introductory remarks, and each attendee (list attached) then introduced themselves. The minutes of the January 7, 2002 meeting were reviewed and approved as written.

II. OLD BUSINESS

LEPC BUDGET REPORT, 2nd & 3rd QUARTERS, FY 2002

L. Nakai provided the following report for the 2nd and 3rd Quarters:

Balance - 9/30/01	\$27,246.06
• 2 nd Quarter Expenditures	
Travel/Notice	3,332.56
• 3 rd Quarter Expenditures	
Travel/Office Supplies/ Notice	397.14
Balance - 3/31/02	\$23,516.36

III. NEW BUSINESS

HSERC MEETING, 1/10/02

L. Nakai briefed members on the 1/10/02 meeting of the HSERC. Bruce Anderson sent a letter to each county mayor shortly after September 11th, urging counties to combine their procurement of WMD agent detection devices in order to take advantage of better deals

Dennis Poma also briefed the HSERC on the leaking chlorine cylinder at the Manele Wastewater Reclamation Facility on Lanai. This was the same presentation given to the LEPC at the November 5th meeting.

LEPC PLAN UPDATE

L. Nakai informed the committee that the contract for services to update the LEPC plan was finalized in April, and that Paul Dixon has begun work to prepare a Hazard Assessment utilizing Risk Management Program guidelines for Chlorine

and Anhydrous Ammonia. The project will focus on Oahu facilities that provide annual reports under HRS 128E, the Hawaii Emergency Planning and Community Right-to-Know Act (HEPCRA). The project will be completed by Fall 2002.

2002 NASTTPO & HMEP GRANTS CONFERENCE

L. Nakai briefed members on the NASTTPO & HMEP Grants Conference that was held at the Ala Moana Hotel during April 8-13, 2002. Of the 153 registrants, 43 were from Hawaii, which included 20 from CLEAN member companies. Conference highlights were the WMD workshop, Cameo/Tier II Submit training sessions, and Abbotville Table Top Exercises. The LEPC Hospitality Suite and Conference Luau held at the Sheraton Moana Surfrider Hotel also were social highlights. A slide show of conference photos was shown. All feedback from attendees on the conference has been very positive and highly complimentary. C. Davis mentioned that congratulatory letters were sent to Mayor Harris.

HAZARDOUS MATERIALS EMERGENCY RESPONSE CAPABILITIES AND ASSESSMENT PROGRAM (CHERCAP) EXERCISE – OPERATION KALAELOA

L. Nakai and T. Seelig provided an overview of Operation Kalaeloa. The exercise will take place on May 22, 2002 in the Campbell Industrial Park area. Based on an industrial accident at AES Hawaii, a chemical release will result in mass casualties in the park, and initiate shelter-in-place actions at Barbers Point Elementary School. Local area sirens and the Emergency Alert System will be tested, along with mass decontamination operations. 13 of 18 Oahu hospitals and volunteer victims from 6 High Schools are participating, and nearly 2000 personnel will be involved in this island wide exercise.

C.L.E.A.N. UPDATE

J. Vinton informed the LEPC that the revised Campbell Industrial Park Emergency Resources Guide was recently distributed. CLEAN also presented an emergency planning workshop for CIP Facility Emergency Coordinators on April 17, 2002. CLEAN donated \$31,000 to Barbers Point Elementary School to update their intercom system to enhance communications during a shelter-in-place situation, and will test the system during Operation Kalaeloa.

RISK MANAGEMENT PROGRAM

B. Ekimoto provided some background on the EPA Risk Management Program. She will be conducting audits of facility RMP plans beginning June 2002. HEPCRA reports that facilities provide annually may also be inspected on these site visits. C. Davis invited her to brief the LEPC at the next meeting on the program & its implementation. J. Vinton also asked that she brief the program at the next meeting of the CLEAN Board of Directors.

EXPLOSIVES LEGISLATION

J. Decker discussed legislation that failed to make it through the last legislative session, which would have required reports of explosive inventories. DLIR has

records on 400 permitted magazines, statewide, of which 160 are on Oahu. He described explosive magazines in Kailua and Aiea with 75, 000 lbs and 15,000 lbs respectively of ANFO, the same explosive used in the Murrah building bombing in Oklahoma City, to illustrate public safety threats to our community.

DLIR is only involved in the design and placarding of magazines, and does not maintain inventories of explosives. There is no current requirement for annual inventories since the Governor repealed the law requiring those reports a few years ago. Although a few companies continue to provide inventory reports voluntarily, the vast majority of the permitted magazine owners do not. The legislation this year attempted to restore these annual reports, but the legislation did not make it out of committee. Also, the potential 5% budget cut is threatening to eliminate DLIR's Certificate of Fitness program, which will mean that there will be no oversight over the sale and use of explosives in the State.

C. Davis stated that he would inform the Fire Chief of the situation, and plans to support future legislation to establish explosive inventory reporting.

WMD DETECTION EQUIPMENT DISPLAY

C. Davis discussed and demonstrated the Guardian BTA (Bio-Threat Alert) Test Strip System currently being used by HFD. It provides a field presumptive test that is 95% accurate for potential biological threats. Confirmatory lab testing is required to confirm field positive tests. The City has developed a Mobile Lab using PCR DNA analysis technology that would conduct tests of the field presumptive positives, and has also acquired BioCapture BT 550 Aerosol Sample System, which basically collects samples that would be tested on the BTA test strip. LEPC members then viewed the Mobile Lab and its PCR DNA analysis system.

IV. OTHER BUSINESS/OPEN DISCUSSION

A. Keith discussed the recent power outage that occurred on 5/10/02. AES Hawaii tripped off line during the afternoon peak hours, which caused programmed outages throughout Oahu. Andy offered to conduct a tour of HECO power facilities for interested members. He will provide a couple of dates, and interested members will sign up for the tours.

V. SCHEDULE NEXT MEETING

The next LEPC meeting will be held scheduled shortly before the August HSERC meeting. The meeting adjourned at 10:56 A.M.

Respectfully Submitted,



Leland A. Nakai
LEPC Coordinator

Attachment

**HONOLULU LOCAL EMERGENCY PLANNING COMMITTEE MEETING
MAY 13, 2002
HUMAN RESOURCES CONFERENCE ROOM**

ATTENDANCE LIST

VOTING MEMBERS:

Carter Davis	HFD
Leland Nakai	OCDA
Randall Lee	Environmental Services
Steven Ogata	Department of Agriculture
Jim Vinton	Tesoro Hawaii
Roy Yamamoto	Healthcare Ass'n of Hawaii
Shirley Zhai	BEI
Paul Epstein	HPD
Donna Maiava	DOH
Andy Keith	HECO
Ed Yoshida	DFM
Glenn Moir	DTS
Lope Salvatierra	Enterprise Services

NON-VOTING MEMBERS:

Denis Shimamoto	HEER
Beryl Ekimoto	HEER
Michele Chang	MCBH
William McGinnis	USAGHI Environmental
Latarsha McQueen	USCG MSO
James Decker	DLIR HIOSH
Terry Seelig	HFD

Hazardous Materials Classes
Class Schedule 2002 (Projected)
Revised As of May 23, 2002

Course: **Technician Refresher (COMPLETED)**
Date: January 26, 2002
Location: Oahu; Honolulu Fire Department Training Center
Instructor: John Bowen

April 8 – 13, 2002, NASTTPO 2002 Conference in Honolulu

Course: **Awareness Initial**
Date: June 2002
Location: Kauai
Instructor:

Course: **Awareness Initial**
Date: June 2002
Location: Maui
Instructor:

Course: **Awareness Refresher**
Date: June 2002
Location: Kauai
Instructor:

Course: **Technician Refresher**
Date: July 8, 2002
Location: Kauai
Instructor: John Bowen

Course: **Technician Refresher**
Date: TBD 2002
Location: Oahu; Honolulu Fire Department Training Center
Instructor:

Course: **Technician Refresher**
Date: TBD 2002
Location: Maui
Instructor:

Course: **Awareness Initial**
Date: June 10, 2002, 8:00 am – 5:00pm
Location: Hawaii County Police Department
Instructor: John Bowen

May 22, 2002, HAZMAT CHER-CAP Field Exercise “Operation Kalaeloa”

Course: **Awareness Initial**
Date: June 7, 2002, 8:00 am – 5:00 pm
Location: Kona Airport
Instructor: John Bowen

Course: **Awareness Initial (OCDA)**
Date: July - August 2002
Location: Oahu
Instructor:

Course: **Awareness Refresher (OCDA)**
Date: July - August 2002
Location: Oahu
Instructor:

Course: **Technician Refresher**
Date: June 2002
Location: Oahu; Honolulu Fire Department Training Center
Instructor:

Course: **Awareness Initial (OCDA)**
Date: July - July 2002
Location: Oahu
Instructor:

Course: **Awareness - Refresher (OCDA)**
Date: July - August 2002
Location: Oahu
Instructor:

Course: **Table Top Exercise Design**
Date: July 31 - Aug 1, 2002
Location: Honolulu Community College, Bldg 4, Room 23-B
Instructor: Ron Alves

Course: **Awareness Initial (OCDA)**
Date: July - August 2002
Location: Oahu
Instructor:

Course: **Awareness Refresher (OCDA)**
Date: July - August 2002
Location: Oahu
Instructor:

Course: **Technician Refresher**
Date: August 2002
Location: Hilo
Instructor:

Course: **Technician Refresher**
Date: August 2002
Location: Kona
Instructor:

Course: **Technician Refresher**
Date: August 2002
Location: Oahu; Honolulu Fire Department Training Center
Instructor:

Course: **Awareness Initial (OCDA)**
Date: September 2002
Location: Oahu
Instructor:

Course: **Awareness Refresher (OCDA)**
Date: September 2002
Location: Oahu
Instructor:

Course: **Technician Refresher**
Date: September 2002
Location: Maui
Instructor:

Course: **Technician Refresher**
Date: September 2002
Location: Oahu; Honolulu Fire Department Training Center
Instructor:

Course: **Technician Chemistry (80-Hours)**
Date: September 9 – 20, 2002
Location: Hilo
Instructor: John Bowen & Doyle Manke

Course: **Technician Tactics (80-Hours)**
Date: October 14 – 25, 2002
Location: Hilo
Instructor: John Bowen & Myron Yoshioka

Other Training

Course: **Inland Search & Rescue (SAR)**
Date: February 3 – 7, 2003
Location: TBD, Honolulu
Instructor: National Search and Rescue School

April 18, 2002

To: Curtis Martin
From: Denis M. Shimamoto *DMS*
Subject: FY 03 HSERC Budget

Collections from the TIER II Reports:

1/01/01 – 06/30/01 = \$39,800

7/01/01 – 12/30/01 = \$30,200

Total \$70,000

FY 01 Kauai HMEP Planning Grant Project = \$17,645

Reimbursement from DOD for Kauai HMEP Planning Grant Project (80%) =
\$14,116 but credited on February 2002. These funds will be available for
FY 04.

Total Tier II collections = \$70,000
Less Kauai HMEP Planning Grant Project = \$17,645

Funds available for FY 03 HSERC Budget = \$52,355

To attend LEPC meetings: \$3,036
M2K HazMat Explo 2002: \$1,545
20% Match for the HMEP Planning Grant: \$10,752
(Based on last years grant of \$43,006)

Funds available for distribution to the LEPCs:

\$52,355
-3,036
-1,545
-10,752

\$37,022

TIER II Reporting Facilities by Counties for the 2000 calendar year:

City and County of Honolulu:	274	(44.4%)
County of Maui:	108	(17.5%)
County of Hawaii:	160	(25.9%)
County of Kauai:	75	(12.2%)

Tab F Project Narrative for Upcoming Activities

Planning Grant

The planning grant funds will be used for the following activities.

1. Annual HazMat Exercises for each of the LEPCs.
2. Update of Emergency Operation Plans
3. LEPC Support
4. M2K HazMat Explo 2002 Convention in Las Vegas, Nevada, December 2-6, 2002

Since Hawaii is an island state, meeting to share and discuss information involves substantial traveling.

HSERC meetings are held quarterly. Each LEPC should follow a similar schedule. A representative from each of the LEPCs attends each HSERC meeting. The HEP CRA Coordinator, and a State On Scene Coordinator with primary responsibility for the county, attends each LEPC meeting. Each county encompasses different islands. The only way to reach another island, in a timely manner, is by air. In the Fiscal Year 02-03, a one-way coupon cost \$42.00; a car rental coupon cost \$35.00; meal allowance of \$20.00 and parking of \$10.00.

LEPC Meetings

Airfare: We are planning for four meetings annually. There are four counties. Two HEER representatives fly to twelve of the sixteen meetings. $2 \times 12 \times \$84 = \$2,016.00$
Rental Car: $12 \text{ meetings} \times \$35 = \$420.00$
Meal Allowance: $2 \times 12 \times \$20 = \480.00
Parking: $12 \times \$10 = \120.00
Total: \$3,036.00

M2K HazMat Explo 2002 Convention in Las Vegas, Nevada, December 2-6, 2002

Airfare: \$500.00
Registration: \$95.00
Per diem: $7 \times \$130.00 = \910.00
Fare from airport to hotel: $2 \times \$20.00 = \40.00
Total: \$1,545.00

The total cost for the HSERC and LEPC activities for the year is \$4,581.00.

October 5, 2001

HAWAII STATE EMERGENCY RESPONSE COMMISSION

FY 01-02 BUDGET

Allocated Funds \$69,700

Travel \$ 5,841

LEPC Funding \$53,342

Honolulu $\$5,000 + .43(\$33,342) = \$5,000 + \$14,337 = \$19,337$

Hawaii $\$5,000 + .28(\$33,342) = \$5,000 + \$ 9,337 = \$14,336$

Maui $\$5,000 + .17(\$33,342) = \$5,000 + \$ 5,668 = \$10,668$

Kauai $\$5,000 + .12(\$33,342) = \$5,000 + \$ 4,001 = \$ 9,001$

HMEP Planning Grant Match \$10,517

HMEP Planning Grant (From Federal DOT) \$42,068

Distribution of Funds $\$42,068 + \$10,517 = \$52,585$

Honolulu \$16,000

Hawaii \$16,085

Kauai \$16,000

Maui \$ 4,500



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
REGION IX
75 HAWTHORNE STREET
SAN FRANCISCO, CA 94105

U.S. EPA Update for Hawai'i SERC

May 23, 2002

New Contact Information: U.S. EPA Region 9 (Pacific Southwest) – All telephone numbers in the Region 9 office changed on Nov. 5. EPA's new number for the regional spill hotline is (415) 947-4400.

National Meetings

NASTTPO 2002 - The Hawai'i SERC, the Honolulu LEPC, the U.S. EPA and FEMA Region 9, among others, co-hosted the 2002 National Association of SARA Title Three Program Officials (NASTTPO) conference in Honolulu, HI on April 8 -13, 2002. Great conference and good work! Mahalo from EPA!

National Governors' Association (NGA) Meeting – Due to the events of Sept. 11, 2001, the NGA conference for the chairs/coordinators of the State Emergency Response Commissions scheduled for Sept. 20-21 in Park City, Utah was rescheduled and held there on May 7-9. One topic of discussion was the role of SERCs and LEPCs in counter-terrorism planning.

New EPA Publications

New Publications – available through 'What's New' on EPA Chemical Emergency Preparedness and Prevention website: <http://www.epa.gov/ceppo/> or Information Hotline 1-800-424-9346.

LEPCs and Deliberate Releases: Addressing Terrorist Activities in the Local Emergency Plan (August 2001). In recent years, the threat of incidents involving chemical and biological materials has increased. This fact sheet discusses how LEPCs can incorporate counter-terrorism issues when they review and update their local plans.

Chemical Safety Alert -- "Chemical Accident Prevention: Site Security" (February 2000). As a precaution during this heightened state of alert, the U.S. EPA in coordination with the U.S. Dept. of Transportation (DOT) and the Federal Bureau of Investigation (FBI) suggests that those who manufacture, distribute, transport or store hazardous chemicals should be especially vigilant regarding the physical security of those chemicals. In addition to this EPA advisory, DOT has produced a separate advisory for transporters, available by contacting DOT at (202) 366-6525. The FBI requests that you expeditiously report any threats or suspicious behavior to your local FBI field office.

LEPC Video: "Guarding the Safety of Your Community" (March 2002) – A brand-new, 23-minute video for LEPCs was produced by EPA Region 3 (Mid-Atlantic Region) and a copy was recently forwarded to every LEPC chair in the U.S. If an LEPC did not receive the video or needs an extra copy, please contact Al Brown, EPA Region 3 at (215) 814-3302.

New EPA Publications

NRT-1 Hazardous Materials Planning Guide (Updated 2001) - The 2001 update of the 1987 Hazardous Materials Emergency Planning Guide (NRT-1, "Orange Book") contains updated references to guidance on developing state and local emergency response plans. This updated version from the National Response Team includes guidance on integrating LEPC plans with planning requirements – including counter-terrorism.

List of Lists – EPA's October 2001 Consolidated List of Chemicals Subject to the Emergency Planning and Community Right-to-Know Act (EPCRA) and Section 112(r) of the Clean Air Act (also known as the List of Lists) is available. New searching options include search by name or by CAS number. The document is also available in PDF. It can be located on the CEPPPO website at: <http://www.epa.gov/ceppo/ap-otgu.htm>

New EPA Publications (continued)

Tier 2 Submit Fact sheet (December 2001) – Tier2 Submit is the free personal computer software developed by EPA and NOAA for use by facilities in submitting Tier II reports in states where this software meets state reporting requirements. Tier II reports required under the Emergency Planning and Community Right-to-Know Act (EPCRA) provide state and local officials and the public with specific information on certain chemicals that are present at facilities during the previous calendar year.

Other Recent Publications of Interest:

"Site Security Guidelines for the U.S. Chemical Industry," developed by a group of company security professionals and designed specifically for the chemical industry, can help member companies build upon their existing security programs. The guidelines outline typical elements of a good security program and suggest security practices that managers can consider and tailor to their facilities' particular circumstances. This includes information on employee and contractor security issues, risk assessment, prevention strategies, training, emergency response and crisis management, and physical and cyber security issues. This document is available in the American Chemical Council website at: <http://www.americanchemistry.com/>

The National Institute of Chemical Studies (NICS) training materials and reports for EPA include a "Sheltering-in-Place" training CD which is available from the NICS website (www.nicsinfo.org). Two reports are also available: (1) **Sheltering in Place as a Public Protective Action**, and (2) **Local Emergency Planning Committees and Risk Management Plans: Encouraging Hazard Reduction**.

EPCRA Enforcement Alert:

As part of last year's EPA Emergency Planning and Community Right-to-Know Act (EPCRA) enforcement settlement against Brewer Environmental Industries in Hawai'i, the company donated an estimated \$137,000 in equipment to the county fire departments.

Computer Aided Management of Emergency Operations (CAMEO)

A New, Expanded, Faster CAMEO System is now available.

It can be downloaded from <http://www.epa.gov/ceppo> using the 'What's New' button.

**CONGRATULATIONS TO EVERYONE FROM EPA ON THE
SUCCESSFUL OPERATION KALAELOA HAZMAT RESPONSE EXERCISE HELD MAY 22, 2002
AT CAMPELL INDUSTRIAL PARK**

MAHALO FOR ALL YOUR HARD WORK!

CEPP Program Contact / Pacific Southwest Region

For more information about U.S. EPA's Chemical Emergency Prevention and Preparedness program in Hawai'i, please contact:

Michael Ardito at 415/972-3081 or by email at: ardito.michael@epa.gov