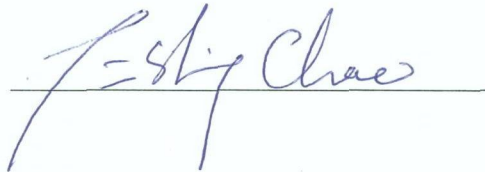


**HSERC MEMBERS OR THE VOTING REPRESENTATIVES'  
SIGN-IN SHEET FOR December 17, 2009**

Dean M Yoshizu  
Dept. of Agriculture  
Board of Agriculture

---

Tin Shing Chao  
Manager  
Occupational Safety and Health Division  
Department of Labor and Industrial Relations



---

Henry Silva  
Hawaii Representative/LEPC Chairperson  
Hawaii County Fire Department

Captain Carter Davis  
Honolulu Representative/LEPC Chairperson  
Honolulu Fire Department



---



---

Albert Kauai  
Kauai Representative/LEPC Chairperson  
Kauai Fire Department

Scott Kekuewa  
Maui Representative/LEPC Chairperson  
Maui Fire Department



---

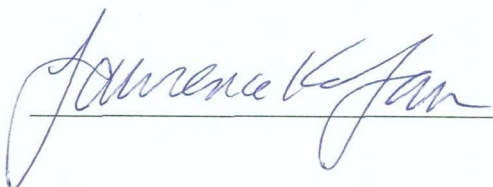


---

Laurence K. Lau  
Deputy Director, Environmental Health  
Department of Health

Katherine P. Kealoha  
Director  
Office of Environmental Quality Control

---



---

**HSERC MEMBERS OR THE VOTING REPRESENTATIVES' SIGN-IN  
SHEET FOR December 17, 2009**

Chris Takeno  
Hazardous Materials Officer  
Department of Transportation

---

Edward Teixeira  
Vice Director  
State Civil Defense  
Department of Defense

Jay Maddock, Ph.D.  
Director  
Office of Public Health Studies  
University of Hawaii at Manoa

*for Christine Chung*

---

*Rob Juarez*

---



## **HSERC MEETING #77 - For Larry**

1. Handouts on table
2. Sign-up for E-Plan System Security Plan Report, three examples provided. Sharon will e-mail document to you.
3. Mike Cripps would like to talk about Fire Works under Other Business.
4. Jan has advised that March 18<sup>th</sup> and 25<sup>th</sup> are open.

**\*\* HEER OFFICE PARTY TODAY AFTER MEETING**

LINDA LINGLE  
GOVERNOR OF HAWAII



LIEUTENANT GOVERNOR'S  
OFFICE

STATE OF HAWAII  
DEPARTMENT OF HEALTH

'09 DEC 11 P2:30

P.O. BOX 3378  
HONOLULU, HAWAII 96801

CHIYOME L. FUKINO, M.D.  
DIRECTOR OF HEALTH

In reply, please refer to:  
HEER OFFICE

HAWAII STATE EMERGENCY RESPONSE COMMISSION  
MEETING #77

Thursday, December 17, 2009 from 8:30 a.m. to 10:30 a.m.

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

AGENDA

- 1) 8:30 Call to Order  
Approval of Minutes from Mtg #76  
Announcements  
Laurence Lau, Deputy Director for Environmental Health
- 6) 8:40 Update On Harbor Improvement  
and Development Plan, Fire Fighting,  
Spill Prevention and Hazardous Release  
DOT Harbors, Fred Nunes
- 7) 9:00 Future of State On-Scene Coordinators  
And Their Importance On Long Term  
Spill Mitigation – 128D  
Carter Davis Honolulu LEPC, LEPC's
- 9:20 BREAK
- 2) 9:30 LEPC Updates  
Henry Silva, Hawaii LEPC Representative  
Albert Kauai, Kauai LEPC Representative  
Scott Kekuewa, Maui LEPC Representative  
Carter Davis, Oahu LEPC Representative
- 3) 9:45 EPA Update  
Mike Ardito, USEPA Region 9
- 4) 9:55 HMEP  
State Civil Defense
- 5) 10:05 HEPICRA Administrative Rules  
Update, Discussion and Decisions  
HEER, Tetra Tech
- 8) 10:15 Other Business  
IT Services  
HSERC, HEER
- 9) 10:25 Schedule next HSERC meeting

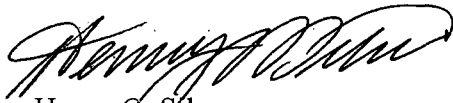
Barry Periatt- County of Hawaii, Civil Defense  
John Jack Roney- Citizen Member  
Paul Smith- Hamakua Energy Partners  
Elton Sugamuma- State of Hawaii, D.O.T Harbors  
Larry Weber- County of Hawaii, Police Dept.

Reviewed and approved by,

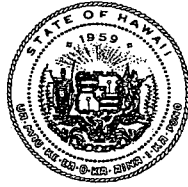


William P. Kenoi  
Mayor, County of Hawaii

Submitted by,



Henry G. Silva  
Chairman, Hawaii County LEPC



STATE OF HAWAII  
DEPARTMENT OF HEALTH

P.O. Box 3378  
HONOLULU, HAWAII 96801-3378

In reply, please refer to:

EHA/HEER Office

HAWAII STATE EMERGENCY RESPONSE COMMISSION  
MEETING # 76

Thursday, September 3, 2009 from 8:30 a.m. to 10:00 a.m.

Department of Health  
919 Ala Moana Boulevards, 5<sup>th</sup> Floor  
Honolulu, Hawaii 96814

Attendees

Voting: Laurence Lau, Department of Health; Carter Davis, Honolulu LEPC; Tin Shing Chao, Department of Labor and Industrial Relations; Henry Silva, Hawaii County LEPC; Scott Kekuewa, Maui LEPC; Albert Kauai, Kauai County LEPC; David Smith, State Civil Defense, Department of Defense; Rebecca Alakai, Office of Environmental Quality Control; Chris Takeno, Department of Transportation; Dr. Deborah Juarez, Office of Public Health Studies

Non-Voting: Sharon Leonida, Department of Health, HEER Office; Beryl Ekimoto, Department of Health, HEER Office; Keith Kawaoka, Department of Health, HEER Office; Curtis Martin, Department of Health, HEER Office; Mike Cripps, Department of Health, HEER Office; Paul Chong, Department of Health, HEER Office; Rob Nakama, USCG Sector; Teress DeBerard, USCG Sector

1. Larry Lau called the meeting to order 8:30 a.m.
  - 1.1 Concerned about voting issues, rules, item #5. Advance item #5 after approval of minutes.
  - 1.2 Approval of minute. Carter: **moved to adopt the minutes from meeting #75. Tin Shing Seconded. Minutes adopted.**
  
5. HEPCRA Administrative Rules Update:
  - 5.1 Tetra Tech is not here, Sharon explained changes; clarifications, word changes, addition of statue used for references. Larry had wanted others on commission to see matrix on changes to draft rules. Most of changes for style or clarifications. Attorney General's Office had changes to make rules more consistent, readability better. There is a strong need to allow for future electronic reporting. Carter added that commission had given Larry the authority to make small changes and have rules go on to Public Hearings. Larry to consult with AG's office if change needed or just add in general language that electronic reporting maybe required in the future. Gives us authority to make changes in future without having to come back and redo rules. HEER staff to make appointment with Larry's secretary for following week before he leaves.

## 2. Local Planning Committee (LEPC) Updates

### 2.1 Hawaii: Henry Silva:

- 2.1.1 LEPC meeting was held on July 30 and August 27, 2009. Two Key items, 1. continue HMEP EOP, Emergency Operation Plan, grant process, plan to put it out to bid by October. The county would like it completed by March. 2. LEPC voted to develop and implement Hawaii LEPC website for county. It is already approved, in process of being put together.
- 2.1.2. Hazmat Incident August 28, at Kawaihae Pier, two pallets of pellet chlorine that spontaneous ignited in holding area. Discussion of incident, Larry, Henry, Carter, concerning **Hot Wash**, how is an incident reviewed, can HSERC be level where significant incidents that go to an operational level get reviewed? Carter explained that OSHA requires review after hot wash, gave more information. Will share what happened in Honolulu incident when its his turn. Mike Cripps gave example of problem with similar product; shipping document with the products gave emergency response contractor as Chemtrec. Problem/scam, instead of a person to contact they list Chemtrec. When contacted Chemtre replied, the shipper was not listed with them, in this case it was Island Pool & Spa. Carter added that the manufacture may have a contract with Chemtrec, not the wholesaler or shipper.. This needs to be mentioned to Chemtrec when calling them. US DOT was looking at process to come up with National Electronic Shipping Paper process, right now just a paper document. Hopefully enforcement by Federal DOT and Coast Guard, word will get out and will tighten the system. Mike commented that Young Brothers, the receiver of the materials, paid for clean-up.

### 2.2. Kauai: Clifford Ikeda retired, Albert Kauai is Acting Interim LEPC Chair.

- 2.2.1 Updating roster for list of LEPC members, going up to Mayor for approval.
- 2.2.2 Training: Russel from the state gave Radiation class and calibrated their equipment.
- 2.2.3 August 14-17, Exercise – Training. Monday and Tuesday, techs in to familiarization themselves with equipment., monitors, Hazmat I.D. Wednesday - Tabletop, Thursday and Friday, full scale exercise with Pride of America, in Nawiliwili Harbor, Coast Guard, other organizations, also CST. Quite on Kauai for Hazmat incidents.

### 2.3 Maui: Scott Kekuewa:

- 2.3.1. LEPC meeting on June 17, 2009. Next meeting September 22, 2009.
- 2.3.2. Hosting Hazmat I.Q. September 23, on Maui. If anyone interested in attending contact Scott. No incidents, busy battling brushfire. Beryl mentioned he has been promoted to Captain, new station, Kihei.

### 2.4. Oahu: Carter Davis:

- 2.4.1. Last LEPC meeting June 24, 2009, 27 attendees. One new Tech Class, 160 hour training, 28 – 29 completed. Hazmat Tech Refresher, 321 Technicians completed, LSU, Louisiana State University, did CAMEO training; Federal Fire, 93 CST, HEER Office, Hawaii County, Local fire. There were two session, beginning and advance, new Marplot introduced, CAMEO now in two suites, total of four suites; CAMEO Chemical, CAMEO Aloha, Marplot, program is free. Discussion on Campbell Industrial Park, one ton Chlorine cylinder, parts of discussion heard at HSERC before. Follow up to Big Island comment, two AAR, one city conducted with police, Fire, EMS, Tem and one with CLEAN. Issues to address such as: community information, industry information and evacuation . Others are, traffic jams, to get out, plan for CIP showed additional emergency routes. Second exit is a locked gate that would go out to former Barbers Point. New tenet has blocked exit, CIP has to review that issue. Suggestions that landowner look for second entrance and exit, long term plan has an application to look for second entry and exit



that may come from harbor side. Since developed in 1959, only one way in and out. Daytime has over 4,000 employees, never tested special Hazmat siren since it was put on four out of six siren in park. Special Whooping sound that can be activated, only used once in exercise ten years ago. Because of AAR sirens tested on September 1, 2009, at monthly test, city will test Special Whoopie Hazmat sound, it will be for sirens within CIP. Update at next LEPC meeting, addressing evacuation policy, may improve getting people out of park. LEPC meeting is September 18 at City EOC, will discuss recent gas explosion at State Office Tower.

2.4.2. NASTTPO: Two representatives will go in October.

3. EPA Update: Mike Ardito

3.1 Not here, sent handout on table. Sharon mentioned most items were covered previously. Under Electronic Reporting and Signature, states and local agencies can develop their own reporting format including electronic reporting and signature to reduce information management burden on themselves and reporting facilities. We have shared information with Andy Matsumoto.

4. HMEP Update: David Smith

4.1 HMEP Grant turned in, questions came up and had to be clarified, corrected some figures that Charles Rogoff asked for. No major issues, mostly housekeeping. One major clarification, every state allowed to send only two representative to NASTTPO. He has notified the LEPC Chairs about this. Discussion on who it would fund for travel. Carter will use funds from his LEPC, other counties can decide who can use HMEP funds. End of grant period is September 30, Kauai need to submit for training, Tech Training for Hawaii also. May have \$30,000 left, asked Scot t if it's needed for Hazmat I.O.

6. No Break

7. Follow Up On Letters To Fire Council

7.1 Letters sent to each County's Chief that is on the Fire Council. Dale Mosher of HFD, contacted Sharon, he has talked to others that handle training, they were not aware of this courtesy, he will be writing a guideline on this procedure. This is not protocol, possible suggestion on extending invitation to training to other counties. As other people rotate into these training positions, they have something to use as a reference.

8. Follow Up On Proxy Voting

8.1 Larry referred to e-mail sent from Kathy Ho about proxy. Discussion with Curtis, Chris, Carter, Larry. Confusion about proxy, Larry had a message from Kathy, will call and speak to her. Will get clarification and distribute it in writing.

9. Other Business: Briefing on Statewide Petroleum Facilities Development Plan

9.1 Chris Takeno sent e-mail inquiring about incident at Hilo Harbor-Barge fire. Answer he received; there is pier improvement plans being worked on. It's possible that county reviews plans, contacted Planning and Design, they gave him a hazy answer. Larry talked to Davis Yogi previously about this, will call him. Letter was to prior administrator. It makes sense to have fire fighting equipment going in if they update the harbors. Discussion with Larry, Chris; Chris had a difficult time finding out about renovation of the Harbors. He will continue to try and gather information, Larry will call Davis Yogi. Mike Cripps had asked Fred Nunes from Harbors to come to the meeting, he did not make it. Mike introduced Lt. Commander Nakama from Coast Guard, they have a Vessel Response Plan, also Marine Salvage and Fire Fighting Plan. He is new to the Planning Section, but, can associate it with the State Harbors Act, it deals with vessels and piers. Commander Nakama briefed HSERC about meeting with HFD. Coast Guard has responsibility to public and port under the Port of Harbors Safety Act; to work

with the first responders in the area of the port and response to any fires on waterway. They do not board vessels to put out fires, except their own vessels. He gave example of agreement that Alaska and Coast Guard have made. Meeting with Honolulu first responders, they have a work group to address issues of fighting fires on vessels, trying to work things out. There is a 2006 Marine Fire Fighting Agreement, it addresses the responsibility of Coast Guard, what's expected of them and local responders should fire occur on vessels here on Oahu waterfronts. Workgroup can forward it to HSERC and people who are concerned. Pier two-Hilo is a Coast Guard regulated facility under MTSA. There is a Security Facility Plan involved, plan is approved by Coast Guard right now. He is a facility inspector, concern is if you modify pier to increase or decrease security level of pier area, Coast Guard wants to be involved and assist whoever will be responsible for maintaining or updating facility security plan. Anything to do with increase of safety, if there is a change in security in that area, Coast Guard should be involved to help get things approved smoothly.

9.2 Homeland Emergency Response Exchange (HERE): Windsor Solutions, application Demo  
Keith gave background information on program. Introduced Simon Watson, Mark Chmarny, they explained about program and some features. Did demo, questions on features. Larry explained about collecting information, Health Department does lots of reporting to EPA. Working for several years to improve and integrate system. Better view of what's going on and providing it to emergency responders. Goal is to improve flow, pull things together more, able to make better and faster decisions. Main electronic tool is the National Environmental Information Exchange Network. EPA administrator wants to finish building network. There are different systems now being used, goal is to move everyone into one system, make things like integration easier. Question on how to protect system asked by Tin Shing. Larry explained how system is protected.

9.3 Briefing on DHS Chemical and HAZMAT Information Reference Portal (CHIRP) Database  
Department of Homeland Security contracted University of Texas at Dallas to gather data from across U.S., we submitted Tier II and got confirmation back that they received data. They will not be sharing this with anyone else. Henry asked about Tier II on local level, how do we do disposal for Tier II? Henry made reference to an item that was forwarded by Sharon about people who are requesting Tier II information and steps to safe guarding information. Check with EPA and State HIPPA for disposal.

10. Schedule next HSERC meeting;

December 17<sup>th</sup>, at 8:30 am. **Scott moved to adjourn, Henry seconded.**

Respectively Submitted,

Sharon L. Leonida  
Environmental Health Specialist III

**HONOLULU LOCAL EMERGENCY PLANNING COMMITTEE  
MEETING**

9:00 A.M. – 11:00 A.M.  
December 16, 2009

Emergency Operating Center  
Department of Emergency Management  
650 South King Street  
Honolulu, Hawaii 96813

**AGENDA**

**1. Call to Order**

- Opening Remarks & Introductions
- Discussion/Approval of Minutes from September 18, 2009 Meeting

**2. Old Business**

- LEPC Budget Report, 1st Quarter FY 2010

**3. New Business**

- HSERC Discussion for December Meeting
- Training Activities & HMEP Grant update
- CLEAN Update
- Review of EPCRA/HEPCRA & State/County Environmental Emergency Response Laws
- NASTTPO MidYear Meeting

**4. Other Business/Open Discussion**

- Training Equipment Purchase for HFD
- ASTI Ammonia Training
- Mike Ardito, EPA
- Chair's Status

**5. Schedule Next LEPC Meeting/Adjournment**

## HI Environmental Emergency Response

- First responders are provided emergency mitigation authority via county charters
- HRS Title 10 Chapter 128D
  - Establishes OSC, gives them authority to manage clean up and access to state spill response funds
  - Designates the Responsible Party
  - Address Public Health Issues
  - Site Restoration Standards
  - Cost Recovery

## OSHA, HIOSH - HAZWOPER

- 29 CRF 1910.120 & HIOSH Chapter 99
  - Site Safety Plans or SOP/SOGs
  - Scene Management System (ICS)
  - Incident Commander & Safety Officer
  - Training (Initial & Refresher
    - Awareness, Operations, Technician, Specialist, Scene Commander
  - Medical Monitoring Program
  - Proper PPEs to perform stated mission



## Hawai'i County Local Emergency Planning Committee

c/o Hawai'i District Health Office  
1582 Kamehameha Avenue  
Hilo, Hawai'i 96720

---

December 6, 2009

To: Mr. Laurence K. Lau, Chair  
Hawaii State Emergency Response Commission  
Department of Health  
919 Ala Moana Boulevard, 5<sup>th</sup> Floor  
Honolulu, Hawaii 96814

From: Henry G. Silva, HSERC Commissioner  
Hawaii County LEPC  
c/o Hawaii District Health Office  
1582 Kamehameha Avenue  
Hilo, Hawaii 96720

Subject: Hawaii County LEPC Committee

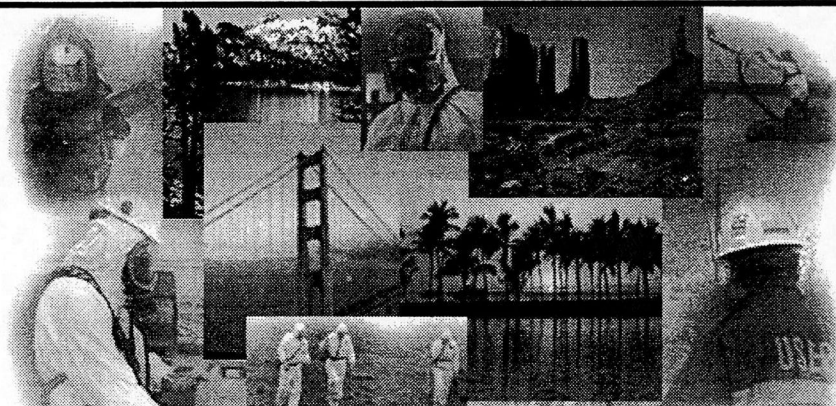
Aloha Mr. Laurence K. Lau,

On December 3, 2009; the Hawaii County L.E.P.C met and voted, to update its membership. These submitted names, will replace any existing voting members or appointment to the Hawaii County LEPC.

Henry G. Silva-	Chairman, Hawaii County L.E.P.C
John Bowen-	Vice Chairman, Hawaii County L.E.P.C
Jason Armstrong-	Media
Tracy Aruga-	Hospital- Hilo Medical Center
Hunter Bishop-	County of Hawaii, Mayor's Office
Newton Inouye-	State of Hawaii, District Health Office
Gerald Kosaki-	County of Hawaii, Fire Dept. Special Operations
Kaipo Parish-	County of Hawaii, Fire Dept. HAZMAT
John Peard-	State of Hawaii, HEER Office



United States  
Environmental Protection Agency  
Pacific Southwest Region



**EMERGENCY PREVENTION, PREPAREDNESS, AND RESPONSE  
PROGRAM UPDATE FOR HAWAI'I SERC  
MEETING IN HONOLULU ON DECEMBER 17, 2009**

---

## **PREVENTION, PREPAREDNESS AND RESPONSE ACTIVITIES**

### **Jared Blumenfeld Selected as New EPA Regional Administrator**

Last month U.S. EPA Administrator Lisa Jackson announced the selection of Jared Blumenfeld to be the Agency's Regional Administrator for the Pacific Southwest. He will begin his new assignment the first week of January and serve as liaison to state and local government officials.

Jared is currently the Director of the San Francisco Department of Environment where he spent eight years as the primary environmental decision-maker for 28,000 city staff and a \$6.5 billion budget. He also managed the San Francisco Recreation and Parks Department which encompasses 242 parks and recreational centers including Golden Gate Park. He is a founder of the Business Council on Climate Change, an organization that unites local businesses around the challenge of climate change. His varied experiences also include leading the first United Nations World Environment Day hosted by the United States and held in San Francisco, directing international initiatives to protect 8 million acres of wildlife habitat, and editing an annual report on international environmental case law at Cambridge University. Blumenfeld received his law degrees at the University of London and the University of California.

### **Toxic Release Inventory Data Released for 2008**

Facilities operating in Hawai'i increased toxic releases by five percent in 2008 compared with 2007, according to the latest data provided to the public earlier this month. The data comes from the EPA's Toxic Release Inventory, commonly referred to as TRI. It is one of the EPA's largest publicly available databases, giving communities valuable information on more than 650 toxic chemicals released by various industries. For more detailed information, you may access the state reports on our regional Web site at [www.epa.gov/region09](http://www.epa.gov/region09) or on the EPA's TRI Web page at <http://www.epa.gov/tri>.

(over)

### **NASTTPO 2010 Annual Conference Near San Luis Obispo, CA**

The 2010 National Association of SARA Title III Program Officials (NASTTPO) annual conference will be held the week of May 10-13 at the Cliffs Hotel in Shell Beach, California near San Luis Obispo and the California Specialized Training Institute. Please check the NASTTPO Web site for additional information when available at <http://www.nasttpo.com/home/>.

### **EPA's OEM Issues "Strategic Direction for Emergency Management Programs 2010 – 2014"**

Now on EPA's Office of Emergency Management (OEM) Web site at [www.epa.gov/emergencies](http://www.epa.gov/emergencies) is a 14-page document called "Strategic Direction for Emergency Management Programs Fiscal Years 2010 to 2014" that includes our chemical emergency preparedness and prevention programs, the oil programs, and homeland security.

### **Frequent Questions Database on OEM Web Site**

On Sept. 9, 2009, the EPA launched the Office of Emergency Management (OEM) Frequent Questions Database on our Web site for use by the general public. The new database can search for frequently asked questions about EPCRA, the Risk Management Plan program, or Oil Pollution Prevention (which includes oil discharge regulations, Spill Prevention and Control Countermeasures, and Facility Response Plans). You can submit your own questions if you do not find a similar one (with an answer) in the database. This application is to make our OEM Web site more user friendly for customers searching for specific information. The link to this tool is available on the OEM Contact Us Web site, under the heading link "View Frequent Questions / Ask a Question," at the following: [http://www.epa.gov/emergencies/contact\\_us.htm](http://www.epa.gov/emergencies/contact_us.htm).

### **CARE Grants Request for Proposals**

The request for proposals for the EPA's Community Action for a Renewed Environment (CARE) grant program is expected to be issued this December. A metropolitan LEPC with the potential for air toxics from facilities, may be interested in applying for one of these grants.

### **EPA's RMP Reporting Center Address Change**

The EPA's Risk Management Program Reporting Center has been moved to a new location in Fairfax, VA. The new mailing addresses for the Reporting Center are:

For the RMP P.O. Box (regular mail):

RMP Reporting Center

P.O. Box 10162

Fairfax, VA 22038

For the RMP physical location (Fed Ex address):

RMP Reporting Center

CGI Federal, Inc.

12601 Fair Lakes Circle

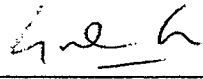
Fairfax, VA 22033

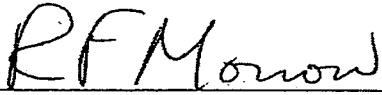
### **EPA Pacific Southwest EPP Program Contact**


For more information about the U.S. EPA's Emergency Prevention and Preparedness program for Hawai'i, you may contact the liaison, Mike Ardito, at (415) 972-3081 or by email at [ardito.michael@epa.gov](mailto:ardito.michael@epa.gov).

# E-Plan System Security Plan

---

Approved By:  Date: 8/20/08  
Dr. Gopal Gupta, Professor and Associate Department Head  
Information Assurance Program Chair  
Erik Jonsson School of Engineering and Computer Science  
The University of Texas at Dallas

Approved By:  Date: Aug 7, 2008  
Richard Morrow, Director  
CyberSecurity and Emergency Preparedness Institute  
The University of Texas at Dallas

Approved By:  Date: 8/8/2008  
Dr. E. Douglas Harris, Associate Dean and Research Professor/  
Executive Director, CyberSecurity and Emergency Preparedness Institute  
Erik Jonsson School of Engineering and Computer Science  
The University of Texas at Dallas



---

## Revision History

The CyberSecurity and Emergency Preparedness Institute is responsible for updating and revising the E-Plan System Security Plan.

Revision No.	Issued Date	Subject	Page No(s).
1.0	May 22, 2003	Initial release	
1.1	March 30, 2005	Changes to address local authorizing officials	All
2.0	August 8, 2008	Update document to reflect current system and contact information	All

## Contact Information

### E-Plan Program

The local, state and federal governments interested in the E-Plan program should contact

Dr. E. Douglas Harris, Associate Dean and Research Professor  
Executive Director, CyberSecurity and Emergency Preparedness Institute  
Address: The University of Texas at Dallas  
800 West Campbell Road  
WT-11  
Richardson, TX 75080-3021  
Telephone: (972) 883-2631  
Fax: (972) 883-4441  
Email: [edh@utdallas.edu](mailto:edh@utdallas.edu)  
Website: <http://csepi.utdallas.edu/>

### About the CyberSecurity and Emergency Preparedness Institute

The CyberSecurity and Emergency Preparedness Institute (CSEPI) is part of the Erik Jonsson School of Engineering and Computer Science at The University of Texas at Dallas (UT Dallas) in Richardson, Texas. It was created to deal with the rapidly growing Homeland Security problems in cyber crime, information assurance, and emergency preparedness. It is one of only a handful of entities of its kind in the United States and UT Dallas has expanded course offerings in Information Assurance, Secure Telecommunications Networks, Cyber Security and Network Security, Data Mining and Multimedia, and Emergency Response Information Systems. The Institute builds on the existing areas of current research successes and highly acclaimed system implementations, for ensuring information security and emergency preparedness. Institute expertise garnered in the process is being leveraged to achieve global recognition in areas vital to national and international security. The Institute has three centers: CyberSecurity Research Center, Global Information Assurance Center, and Emergency Preparedness Center.

### About The University of Texas at Dallas

The University of Texas at Dallas is a dynamic school offering an array of degree programs in engineering, the natural sciences, business and the arts. Our world-class faculty is dedicated to teaching both theory and practice, combining classroom instruction with practical experience in more than two dozen research centers. We have nearly 15,000 students who come from a wide variety of backgrounds, producing a rich atmosphere of ideas and perspectives, and our state-of-the-art facilities include the new \$85 million Natural Science and Engineering Research Laboratory building, which is helping fuel our drive to become a top-tier academic research institution.

**Table of Contents**

**Revision History** ..... ii

**Contact Information** ..... iii

**Sections**

**1.0 E-Plan System Security Overview** ..... 1

**2.0 E-Plan – A Hazardous Materials Emergency Response System** ..... 2

**3.0 Risk Management** ..... 3

**4.0 Security Controls** ..... 6

**5.0 Information Sharing and Public Access** ..... 8

**Appendix A E-Plan Implementation Guide for Authorizing Authority** ..... 9

**Appendix B E-Plan Contingency Operations Procedures** ..... 14

**Appendix C E-Plan Usage Policies and User Responsibilities** ..... 17

**Appendix D E-Plan Acceptable Use Policy** ..... 21

**Glossary Abbreviations and Acronyms**..... 23

## 1.0 E-Plan System Security Overview

E-Plan, a highly-secure web-based hazardous material (HazMat) information delivery system, provides first responders rapid access to the data they need during HazMat incidents or terrorist attacks. Since the E-Plan system stores and dispenses sensitive information concerning hazardous materials, providing security for the data is an absolute requirement. All authorized E-Plan users otherwise involved with E-Plan are carefully screened and their E-Plan user accounts are approved and permitted by the appropriate E-Plan authorizing authorities (see Appendix A). E-Plan system physical security is fully enforced via strict key control and housing the web servers in secure rooms within The University of Texas at Dallas (UT Dallas).

**Fault Tolerance System:** The E-Plan System's main servers are housed in a highly secured, access restricted server room with emergency generator backup power supply. Each main server has redundant power supplies with feeds from dual uninterrupted power supplies (UPS) for power fault tolerance. In addition, each server uses RAID 5 (Redundant array of independent drives) configuration for tolerance against disk failures and data corruption. Failed server components can be hot swapped without disruption of services. The servers themselves are mirrored with redundant backup server hardware in case of a full server hardware failure. The redundant server can be brought online within a few minutes of main server failure.

**Disaster Tolerance System:** The E-Plan System's mirror servers are housed in a secure, remote location. The two sites are connected over network for synchronizing data and configuration. In case of a disaster where the primary server resources are inoperable or unreachable, the remote location can take over the primary server function. Appendix B details the contingency operations procedures.

**Confidentiality and Integrity:** Extreme care is taken to ensure data confidentiality by encrypting information in transit and strictly enforcing usage rules. Prospective users are trained in the appropriate and effective usage of E-Plan (Appendix C) and must agree to the rules for acceptable usage of the system (Appendix D). Data integrity is ensured via several levels of checking mechanisms. Data integrity and confidentiality will be maintained throughout the life of the system.

**Availability and Reliability:** Since E-Plan is accessed at times of emergencies providing information to first responders during accidents, its availability meets or exceeds the industry-standard 99.9%.

**System Monitoring:** System Monitoring programs automatically monitor the health of the E-Plan system, sending text messaging (i.e. SMS) and email notification to system administrators if the system is not accessible.

## 2.0 E-Plan – A Proven Hazardous Materials Emergency Response System

E-Plan is a proven system that provides First Responders and others with on-site hazardous chemical information for facilities around the United States. It utilizes emergency contact and hazardous material information submitted under the U.S. Environmental Protection Agency (EPA) regulations and sends it via the Internet to First Responders just when they need it the most.

E-Plan provides Tier II reporting data and other important information instantly such as

- Maps of the area surrounding a fixed facility showing schools and hospitals,
- Maps of all facilities with a specified hazardous material in specific area,
- Chemical Hazards Response Information System (CHRIS) data,
- Material Safety Data Sheets (MSDS),
- Chemical profiles,
- Emergency Response Guidebook (ERG) pages,
- National Fire Protection Association (NFPA) codes,
- Facility Risk Management Plans (RMPs), and
- Additional documents (e.g., Contingency Plan, photos, site map, etc.) reported by facilities

E-Plan data is stored in redundant servers, which are located in two locked, shielded and secure rooms. Emergency power system (i.e., diesel generator and UPS) and private T-1 connections ensure E-Plan system’s reliability and availability. Security of information is ensured by 128-bit security sockets layer (SSL) encryption.

Since the system stores and dispenses the locations and types of hazardous materials, the security of the data is of primary concern. The general requirements of confidentiality, integrity and availability are as shown in Table 2.1, which summarizes the appropriate levels of control necessary for the different classes of data stored by E-Plan.

Information Category	Confidentiality	Integrity	Availability
Facility Information	Medium	High	High
Contact Information	Medium	High	High
Hazardous Material	High	High	High
MSDS	Low	High	High
Chemical Profile	Low	Medium	Medium
Relevant Links	Low	High	High

Table 2.1 - Acceptable Levels of Security for Information in E-Plan

### 3.0 Risk Management

This section provides an overview of the risk management approach by The University of Texas at Dallas, to include the status of the risk management effort to date, and a description of the risk management strategy to mitigate the impact of the E-Plan system's project-related risks.

UT Dallas desires that confidentiality of data, including facility's hazardous material information, be of paramount importance and that the system design does everything possible to insure that confidentiality of the data is maintained.

#### **Unauthorized physical examination of data in the database**

Two special rooms were constructed to hold all the equipment of the E-Plan computer system. Access to each room is through a locked door equipped with an INTELLIKEY system (IKS). The IKS key carries the access control and personal identity data of the assigned key holder. It cannot be read or duplicated except by authorized personnel equipped with site-specific equipment. Keys are assigned to a limited set of individuals and none of the passkeys used by UT Dallas staff will operate the lock. The IKS key may be programmed with dates to determine a time frame during which it will be allowed to operate. The IKS controller's memory also retains an audit trail of the keys that have been used.

In addition, each room is under video surveillance with a digital video recorder, which provides a multitude of advanced functions including video searches by event, time, date and camera. Moreover, each room is monitored by a web-based camera system that takes pictures of the door shortly after it is opened and sends an e-mail to the UT Dallas CSEPI Management Team, providing a complete visual log of all persons entering the rooms.

The special locked rooms lower the risk of unescorted unauthorized people in the rooms to a level acceptable to the UT Dallas CSEPI Management. The video surveillance procedures assure detection of non-compliance with E-Plan computer system's procedures by UT Dallas employees and also identify any breaches of access.

#### **Lost of equipment/database or other resource due to planned criminal activity**

All the assets of the E-Plan computer system are stored in two special locked rooms, which are not to be shown to the general public. Access to each of these rooms is through a locked door with a high security lock. Unaccompanied access to the locked rooms is granted only to those persons issued a key to these rooms by the UT Dallas CSEPI Management. Persons not authorized access to these rooms may access them only when accompanied by an authorized person (i.e. Key Holder).

The special locked rooms with limited access lowers the risk of loss of assets is acceptable to the UT Dallas CSEPI Management.

### **Physical risk to the servers from the perspective of environment**

The E-Plan computers are triply redundant. That is, there are three identical disks in each machine. Each disk is fully capable of handling the E-Plan computer system's function. Should a disk fail, the other two are available to carry out all tasks of the E-Plan.

The E-Plan main servers are housed in a secure room powered from the local power grid with two levels of power back up. In the event of a power outage, the servers will continue to run uninterrupted due to being protected by redundant battery-based UPS. The UPS also filters the power removing any power spikes or deficiencies providing nominal 110 VAC power to the computers at all times. The UPS keeps the system running for several minutes on its own. Backing up the UPS is a diesel generator that starts momentarily after a loss of power. The diesel generator can supply power indefinitely. Not only are the servers protected by this two level power backup, the private T-1 internet connections and all equipment on that connections are also thus protected.

In addition, the secure room is air-conditioned by two individually operated/redundant private HVAC systems and a humidifier. Temperature is maintained at 68 degrees Fahrenheit and 40% humidity year round. This is the optimum environment for hardware reliability.

Triple-redundant disks and two levels of power back up lower the risk of corrupted data and loss of availability to a level acceptable to the UT Dallas CSEPI Management.

### **Risk of loss of personnel to operate the system**

The software development team has three technically trained individuals familiar with the operating system and Internet utilities to operate the E-Plan computer system. The E-Plan computer system is constantly being automated and simplified to make it easier to use and also to allow lesser-trained individuals to perform the necessary functions.

The software development team can perform all functions required to operate the E-Plan computer system until a replacement for lost personnel can be hired and trained. This level of risk is acceptable to the UT Dallas CSEPI Management.

### **Risk of operational changes**

The operating and development systems are standard well-known and broadly used systems assuring a large pool of knowledgeable personnel. In addition, the E-Plan computer system is constantly being automated and simplified to make it easier to use.

The risk of adding new operator, new machine, or new technique is very low and is acceptable to the UT Dallas CSEPI Management.

**Risk of an intermediate Internet site intercepting E-Plan communication**

Processing transactions securely on the web means that E-Plan system needs to be able to transmit information between its web site and the customer in a manner that makes it difficult for other people to intercept and read. E-Plan is using 128-bit SSL encryption to protect its web transactions. SSL authentication assures authentication on both ends. It not only encrypts the data but also determines whether or not each party (server and client) has the expected authentication. In addition, E-Plan website enables with SSL certificate, which enables encryption of information during online transactions.

The SSL certificate and 128-bit encryption scheme lower the risk of E-Plan web transaction attacks to a level acceptable to the UT Dallas CSEPI Management.

**Risk of authorized users sharing computer equipment with unauthorized users or authorized users accessing information that is not authorized for viewing**

A set of rules and user responsibilities (Appendix C) and acceptable use policy (Appendix D) are distributed to all authorized users of E-Plan. Each user login to E-Plan is treated, as is common web practice, as a session. Session management is accomplished via the use of server memory thus eliminating the need to store any information on the user's computer. Server sessions are a standard solution used by businesses requiring a high degree of security, such as on-line stockbrokers, banks, etc. The server sessions are purged when the user logs out of the system, closes the browser or after a certain period of inactivity.

Since the server sessions are stored in the server's memory instead of the client's memory, it prevents unauthorized access or manipulation by the client. Whenever a request for a page on the server is made by the client, the session managements checks whether a session is present and valid for the user. In the absence of a session, the user is not authorized or restricted to access the page. The session also keeps track of user access level thus restricting access to unauthorized resources.



## 4.0 Security Controls

The UT Dallas E-Plan Team meets monthly to review the E-Plan System's operations and ensure appropriate security initiatives are in place and all UT Dallas employees of the E-Plan System are following all security procedures. The UT Dallas CSEPI Management Team co-ordinates with UT Dallas Information Resources Department to ensure that the E-Plan System is appropriately connected to the UT Dallas computer systems and that appropriate UT Dallas computer system security controls remain in place. The UT Dallas CSEPI Management Team also co-ordinates with the UT Dallas Police Department to ensure that appropriate steps are taken to provide physical security for the computer systems and personnel as well as provide video monitoring of the secure room.

### **Physical Security**

All the servers supporting the E-Plan application are housed in two locked, shielded and secure locations within UT Dallas campus. Theft of application hardware is almost impossible since there are no openings in the four solid walls and the single heavy door is accessed via a high security lock. Entry keys to these rooms are given only to authorized UT Dallas personnel. Written and video records are maintained of all personnel that gain access to the storage locations. Redundant UPS and private T-1 connections ensure E-Plan system's reliability and Internet accessibility. The secure rooms and their operation are certified to ISO/IEC 27001, an international information security standard published by British Standards Institute. Therefore, physical access is completely controlled.

### **Environmental Protection**

All E-Plan computers are protected by redundant UPS. The E-Plan main servers are connected to the building's Emergency Power System. Power flows through the UPS at all times providing filtering of spikes and low voltage. If a power outage occurs, the UPS continues to provide the computers with power and can operate on its own for several minutes. The emergency diesel generator is actuated when the power outage occurs by its automatic transfer switch restoring full power within a few seconds. When grid power is restored, the diesel shuts down. The computers never see the outage .

The E-Plan computers are contained in the rooms where temperature is maintained at 68 degrees Fahrenheit and 40% relative humidity year round. This is the optimum environment for hardware reliability.

Current physical equipment handlers (two system developers and one system administrator) are fully conversant with security processes and ensure system protection.

### **Audit Trails**

System and application audit trails are in place, which enable holding users accountable for their actions when accessing the E-Plan application. These audit trails are also used to identify application performance problems and to provide a recovery path from faults. Both system and application audit trails are reviewed periodically to identify security incidents and possible misuse of, or unauthorized access to, system or application resources. The audit trails for the two categories address the following issues.

- System Audit Trail:
  - Application Manager and Administrator Activities
  - Attempts to log on and log off, together with failures to log on
  - Devices used in the session
  - Functions performed in the session
  - Applications and files accessed in the session
  
- Application Audit Trail:
  - Who viewed the application data
  - Data modified (with before and after snapshots) in the session
  - Reports generated
  
- Common to both trails:
  - Date and time of each critical event
  - User-ID associated with the event
  - Event-initiator (which program, which command, etc.)
  - Event outcome

### **Application Software Maintenance Controls**

E-Plan follows standard software development and maintenance controls and procedures. E-Plan software is maintained in a software management facility to assure the correct modules are used during system builds. Access to the E-Plan System's computers is strictly controlled. No software may be installed on the computers without the authorization of the UT Dallas CSEPI Management.

### **Application Software Configuration Management Controls**

All application modules are maintained using a software module management facility, which guarantees that modules cannot be worked on by more than one person at a time. Software is under tight control utilizing a central management facility. All changed applications are reviewed and tested for proper operation before being installed on the E-Plan System's computers. All modifications to software packages must be approved by the UT Dallas CSEPI Management for proper operation before being installed on the E-Plan System's computers.

## 5.0 Information Sharing and Public Access

The information within the E-Plan application is currently shared between personnel associated with DHS, EPA, state Tier II administrations, UT Dallas, and Weston Solutions Incorporation. All personnel with these organizations accessing and developing the E-Plan system and providing data are well trained in the security procedures currently in place to ensure confidentiality, and are duly authorized for required levels of access.

The general public is not authorized to access the E-Plan application.

## Appendix A: E-Plan Implementation Guide for Authorizing Authority

### I. Introduction

E-Plan is an electronic database managed by The University of Texas at Dallas (UT Dallas). EPA Region 6 has funded the research, development and implementation of E-Plan since from the fall of 2000 through June 2007. The DHS is currently providing funding for completion of E-Plan information on all hazardous sites, dams and bridges in the U.S. and her territories. E-Plan is a secure, web-based hazardous chemical information delivery system for First Responder's use in emergencies. Information provided by E-Plan includes robust chemical hazards database; fixed facility information such as 24-hour emergency contacts, hazardous materials (hazmat) inventories, and building diagrams; and applicable emergency response plans. The information in E-Plan is public information and available via Freedom of Information Act. However, E-Plan access is so highly efficient and complete that it must be protected from access by the general public. This access is what makes E-Plan so valuable to the First Responders so the access mechanism must be restricted.

Much general information such as properties of hazardous chemicals are directly available from E-Plan without a login account. However, log in accounts are required to access specific information such as locations of chemicals within a fixed facility. Login accounts are granted only after being approved by E-Plan Authorizing Authority who know and trust the applicants. Typically, the E-Plan Authorizers are the Local Emergency Planning Committee (LEPC) Chairpersons. This is consistent with the intent of Emergency Planning and Community Right to Know Act (EPCRA), which requires the Governor of each state to designate a State Emergency Response Commission (SERC) to direct and manage the hazardous materials contingency planning effort required of industry and communities.

This document is provided to the state Emergency Management Offices and their county Local Emergency Planning Committees to serve as guidance in determining the E-Plan Authorizing Authority hierarchy in their state (see Figure 1). It is also provided to the federal agencies and their local Emergency Management Offices to serve as guidance in determining the E-Plan Authorizing Authority hierarchy in their agency (see Figure 2).

### II. State Authorizing Authority Hierarchy

Figure 1 describes the overall E-Plan Authorizing Authority hierarchy in a state. The purpose of this approach is to keep the E-Plan authorizing process centralized for users. The goal is to have multiple authorizers in each county, each one representing their specific response discipline (i.e., police, fire, emergency management service). From there, users (from those disciplines) can request user access to the E-Plan system through their appropriate discipline-specific authorizer.

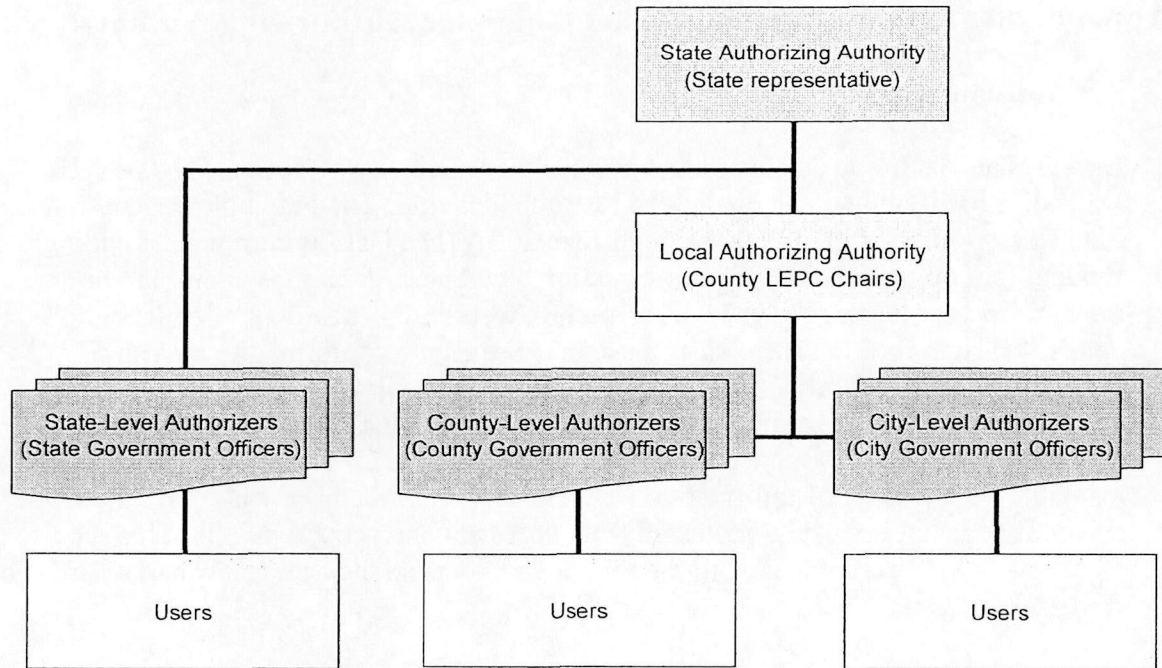


Figure 1 – E-Plan for State and Local Authorizing Authority Hierarchy

#### A. Appointing State Representative

Once a State has determined that they want to have access to the hazmat data in E-Plan and/or to use E-Plan as their Tier II reporting system, they should first identify a KEY PERSON (i.e. State representative) in their state. The State representative then contacts the E-Plan system administrator (UT Dallas) to setup the E-Plan Authorizing Authority hierarchy for their state. The State representative is responsible for managing the entire “Authorizing Authority” hierarchy for that state. The State representative is also responsible for supplying their state Tier II data to be uploaded into E-Plan.

#### B. Approving State-Level Authorizers

The State representative should approve all state-level authorizers. As an example, the following is list of state-level authorizers:

- State Emergency Response Commission (SERC) Chairperson
- SERC Program Coordinator
- Office of Emergency Management – Director, Administrator, SERC Coordinator
- Department of Homeland Security – Director, Administrator, Program Coordinator
- State Fire Marshal Administrator
- State Fire Administrator
- State Tier II Report and/or RMP Report Office Director

- State Department of Environmental Quality Director
- State Department of Environmental Quality Emergency Response Manager
- State Health Department Director
- State Police Superintendent
- State Police Tier II and/or RMP Office Director

### C. Identifying Local Authorizing Authority

The process for identifying the local authorizing authority within a state is as follows.

1. The State representative approves the Chairs of the LEPC's.
2. The State representative sends E-Plan system administrator a list of the current LEPC Chairs in their state.
3. After State representative approves an LEPC Chair for a county, they will approve the Authorizes for their county.

Once an LEPC within a state has determined that they want to use E-Plan, the LEPC Chair should identify the authorizing authorities for their jurisdiction. It is recommended that only a limited number of persons within a county/city be identified as the authorizing authority for their jurisdiction. These persons respond to agency-specific requests (users) to access E-Plan and ensure that access to secure information is maintained and allow for each response discipline (i.e., fire, police, emergency management service) to have an authorizer to confirm access for their respective discipline. As an example, the following is a list of county-level and city-level authorizers:

- County Administrator, County Supervisor
- LEPC Chair; LEPC Coordinator
- County Emergency Management Office – Director, Administrator, Coordinator
- County Homeland Security Representative – Director, Administrator, Coordinator
- County Fire Marshal Administrator
- County Fire Administrator
- County HazMat Team Coordinator
- County Sheriff
- County EMS Coordinator
- Mayor
- Fire Chief
- Hazmat Team Chief
- Police Department – Chief, Emergency Services Coordinator

### III. Federal Authorizing Authority Hierarchy

Once a Federal agency has determined that they want to have access to the hazmat data in E-Plan, they should first identify a KEY PERSON (i.e. Agency representative) in their agency to assume responsibility for reviewing, approving and managing all “Authorizing Authority” applications for that agency. The Agency representative then contacts the E-Plan system administrator to setup the E-Plan Authorizing Authority hierarchy for their agency. The Agency representative is responsible for reviewing, approving and managing all “Authorizing Authority” applications for that agency. Figure 2 describes a typical E-Plan Authorizing Authority hierarchy for a federal agency.

It is recommended that only a limited number of persons within an agency be identified as the authorizing authority for their organization. These persons should be officers that represent their agency and are the lead in decision making on behalf of their respective agency to respond to agency-specific requests (users) to access E-Plan.

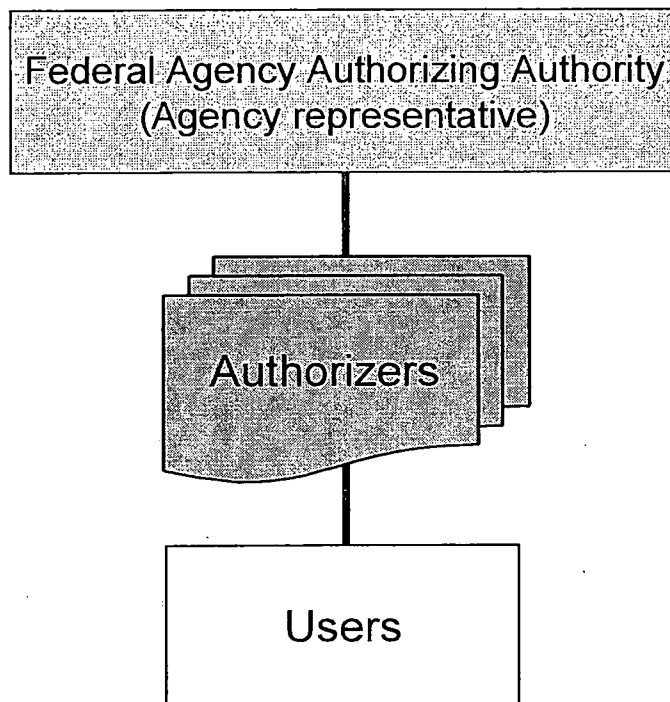


Figure 2 – E-Plan for Federal Authorizing Authority Hierarchy

#### IV. E-Plan Account Request and Approval Process

##### A. Authorizing Authority Account

An E-Plan authorizer must have a valid account on the E-Plan system. The basic process to approve an “E-Plan Authorizing Authority” account would be as follows.

1. Potential “E-Plan Authorizing Authority” must complete and submit the online “Authorizing Authority Account Request” form on the E-Plan home page at <https://erplan.net>. In filing out the form, they must complete the entire form including
  - a. Read, understand, and fill in the “E-Plan Acceptable Use Policy” form
  - b. Select their authorizer from the E-Plan Authorizing Authority list
2. Upon receipt of the complete “Authorizing Authority account request” form, E-Plan will send via e-mail the request for system access to the selected authorizer. The authorizer will back check to see if the request is legitimate and approve or deny as appropriate through local channels.
3. Once approved, a new “Authorizing Authority” account is setup and an e-mail message with the account information is sent to the new “E-Plan Authorizing Authority”.

##### B. User Account

An E-Plan user must have a valid account on the E-Plan system. The basic process to approve an “E-Plan User” account would be as follows.

1. Prospective user must complete and submit the online “User Account Request” form on the E-Plan home page at <https://erplan.net>. In filing out the form, they must complete the entire form including
  - a. Read, understand, and fill in the “E-Plan Acceptable Use Policy” form
  - b. Select their authorizer from the E-Plan Authorizing Authority list
2. Upon receipt of the complete “User account request” form, E-Plan will send via e-mail the request for system access to the selected authorizer. The authorizer will back check to see if the request is legitimate and approve or deny as appropriate through local channels.
3. Once approved, a new “User” account is setup and an e-mail message with the account information is sent to the new “E-Plan User”.



## Appendix B: E-Plan Contingency Operations Procedures

### I. Purpose

The purpose of the E-Plan Contingency Operations Procedures is to support the restoration of operations, computing resources, and critical data in the event of system failures, emergencies, or disaster.

### II. Personnel

The University of Texas at Dallas (UT Dallas) CyberSecurity and Emergency Preparedness Institute (CSEPI) Management Team, Software Development Team, and staff members are responsible for implementation of this E-Plan Contingency Operations Procedure and the restoration of any lost data.

- CSEPI Management Team
  - CSEPI Executive Director
  - CSEPI Global Information Assurance Director
  - CSEPI Program Manager
- CSEPI Software Development Team
  - CSEPI Lead Developer
  - CSEPI Software Developer
  - CSEPI Graduate Research Assistants
- CSEPI staff members

### III. Data Backup Procedure

The main production database is automatically replicated every second onto a standby database in the same room and a backup database on a remote site.

Backups of the E-Plan System are run automatically without operator intervention, according to the schedule set by CSEPI Management Team and implemented by CSEPI Software Development Team.

1. **Daily backup:** A full data backup is taken and stored on the backup server everyday using automatic scripts that are run at 12:00 AM. There are two backup files, one from yesterday and one from the day before yesterday. New copies overwrite these copies on a day-to-day basis.
2. **Weekly backup:** The backup server is configured to operate automatically with backup program running every Saturday at 12 A.M. The backup server will store all 52 sets of weekly backup files, which are appropriately labeled.

3. **Testing the E-Plan System's backup files:** Perform this procedure every six months.
  - a. Call for the key holder to come to the CSEPI Secure Room ECS N3.907
  - b. Log on to the backup computer using root
  - c. Go to the appropriate folder
  - d. Verify the backup files
  - e. Verify consistency of file sizes from backup history
  - f. Log off the backup computer

#### IV Disaster Recovery Plan

1. **Disaster Assessment:** Once a disaster has occurred, UT Dallas CSEPI Management Team will assess the effect of the disaster on the E-Plan System to determine any lost functionality and loss of data. The CSEPI Program Manager will assess the extent of damages to the E-Plan System that enable continuation of its critical operations, and the CSEPI Lead Developer will begin procedures to repair and bring the computer system back online as soon as practical.
2. **Notify Sponsor and Users.** UT Dallas CSEPI Management will notify sponsor and E-Plan users about the system outages and timeframe required for system to be restored.
3. **Personnel Responsibility:** The CSEPI Program Manager is responsible for implementation of this Disaster Recovery Procedure, and the CSEPI Lead Developer is responsible for restoration of any lost data.
4. **Secure Facilities:** In the event of a catastrophic event, UT Dallas CSEPI Management Team will immediately ensure that all facilities housing the E-Plan System remain secure under the circumstances. UT Dallas CSEPI Management Team will limit access to facilities to only the following authorized personnel to assist in disaster recovery:
  - CSEPI Management Team;
  - CSEPI Software Development Team;
  - CSEPI Staff Members;
  - DHS/EPA representatives;
  - UT Dallas Managers and personnel to assist in disaster recovery.
5. **Backup Data:** The CSEPI Program Manager will ensure that the CSEPI Software Development Team has access to any backup media stored onsite/offsite if necessary to restore software, applications, information and data to the E-Plan System.

6. **Systems Architecture and Diagrams:** The CSEPI Program Manager will develop and maintain detailed descriptions of the E-Plan System hardware components to help rebuild the system in the event of disaster. The CSEPI Lead Developer will maintain updated profiles for each system configuration and maintain lists of installed software, including current installed patches, drivers, and operating system distribution media.
  
7. **Recovering the E-Plan System's database:** Perform this procedure only as instructed by the CSEPI Executive Director and/or CSEPI Global Information Assurance Director.
  - a. Call for the key holder to come to the CSEPI Secure Room ECS N3.907
  - b. Log on to the backup computer using root
  - c. Go to the appropriate folder
  - d. Verify the backup files
  - e. Restore database through the network
  - f. Log off the backup computer

## Appendix C: E-Plan Usage Policies and User Responsibilities

### 1. Application Usage Policies

Security of the data in E-Plan requires that users understand the need for security and use the system only in ways that provide security for the data. Training materials are provided to define the acceptable use of the system and each authorized user agrees to use the system as defined by the security policies.

### 2. E-Plan User Responsibility Violations

The Acceptable Use Policy (Appendix D) details the range of possible actions that may result due to violation of the usage policies. All E-Plan users must ensure that the application and its data are protected from loss, misuse, and unauthorized access or modification. It is paramount, especially so after 9/11, that sensitive information in E-Plan be protected.

All E-Plan users are responsible and accountable for their use of the application and its data. Failure to follow the usage policies set-forth in the Acceptable Use Policy (Appendix D) may result in suspension of access privileges.

Note: Consequences of non-compliance are based on the severity of the violation, at the discretion of the project responsible officials and due process of the applicable laws. In addition, especially for the unauthorized disclosure of confidentially sensitive data, there may be criminal and civil penalties, including fines and/or prison terms.

### 3. E-Plan User Responsibilities

- Attend E-Plan application use training sessions
- Be familiar with all security policies and practices involving the E-Plan application, especially those for confidentially sensitive information
- Maintain security for the application by correctly using established security mechanisms and practices when accessing the E-Plan application
- Notify the appropriate personnel of security incidents immediately
- Notify the E-Plan operation manager when authorized users have been terminated from the position that authorized them for use of E-Plan

### 4. Policies for Using E-Plan Data

- Users are not to attempt to view, change, or delete data unless they are authorized to do so
- Users may not use their system privileges to obtain data/files or run applications for anyone who is not authorized to do so
- Users must control access to their personal computer and not permit unauthorized access to occur
- Users should use a screen saver with a password set it to display after 2 minutes of inactivity

### 5. Acceptable Passwords

- Use at least 8 characters in the password, with a mix of alpha, numeric, upper case, lower case and special characters
- Passwords that are easy to guess, such as family names, birthdays, or regular English words found in any dictionary should not be used
- Use different passwords for different applications
- Commit passwords to memory, instead of recording it; or keep on person if recorded
- Passwords should not be reused

### 6. Usage Policies for Login E-Plan Data

- These policies apply to the data accessible on E-Plan that require a login
- Ascertain that only authorized personnel can access E-Plan data, whether on screen in a monitor or on paper in a file
- Position workstation/computer screens away from doors, windows and heavily traveled areas
- Destroy printed copies of E-Plan data by shredding
- Do not save data to hard drives or diskettes

**7. Usage Policies for Protecting PCs and Workstations**

- Follow all general virus protection procedures
- Regularly scan for virus infection using latest available virus software
- Do not use disks from other machines without first scanning them

**8. E-Plan Operation Manager Responsibilities**

- Recommend and apply security mechanisms; enforce security policies outlined here
- Conduct periodic security reviews to ensure adherence to security policy
- Ensure that the E-Plan application documentation is complete and up-to-date
- Ensure that the application and data are regularly backed up according to the E-Plan Contingency Operations Procedures (see Appendix B)
- Assure that backups are protected to the same levels of confidentiality and integrity requirements as the application and the E-Plan data
- Ensure that the backups reside off-site from the application location
- Periodically review application audit trails
- Notify appropriate personnel on suspicion/detection of violations
- Provide and maintain passwords and password files respectively
- Ensure enforcement of authentication procedures for adding new users

**9. E-Plan Operation Maintenance Staff Responsibilities**

- Ensure that source code and data are modified only by authorized personnel
- Follow all security guidelines and policies, in addition to following user rules
- Recommend additional security controls as necessary
- Ensure testing of code with data not deemed confidential and sensitive

- Test all deployed code for technical and operational security
- Notify appropriate personnel upon suspicion/detection of violations

### **10. Training**

All individuals authorized to access E-Plan are provided with training prior to gaining access. This training procedure provides all personnel accessing E-Plan with the knowledge and skills required to use the application securely. Training is limited to ensuring secure usage of E-Plan. Each user is trained only on those aspects of the application essential to carry out the tasks assigned.

### **11. Personnel Security**

The E-Plan application processes information that requires a high degree of availability and integrity. With these stringent requirements in view, the following three categories of personnel security controls are: Separation of Duties, Assignment of graduated and minimum required Privileges, and User Accountability.

### **12. Contingency Planning**

Appendix B describes the Contingency Operations Procedures that assure E-Plan can continue operating in the event of an emergency.



*When every second counts...*

# Acceptable Use Policy

This Acceptable Use Policy is effective as the date of last signature below and by \_\_\_\_\_ (User). Moreover, the User recognizes and agrees that the E-Plan account issued to the User is the sole and exclusive property of E-Plan and may be revoked at any time without advance notice to the User and at the sole discretion of E-Plan.

The Acceptable Use Policy defines the guidelines and specifies the actions that are prohibited by E-Plan regarding the use of the E-Plan Emergency Response Information System. E-Plan reserves the right to modify the Acceptable Use Policy at any time and without notice, effective upon the posting of said changes at URL: <https://erplan.net/eplanacceptableusepolicy.pdf>.

The User must read, understand, initial, and abide by the Terms and Conditions as set forth below. By signature hereto, the User agrees to be bound by the Terms and Conditions contained herein by E-Plan.

## **Illegal Action**

Accept

The E-Plan Emergency Response Information System may only be used for lawful purposes. Transmission, distribution, or storage of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret, or other intellectual property right used without proper authorization, and material that constitutes an illegal threat or violates export control laws.

## **System and Network Security**

Accept

Violations of system or network security are prohibited and may result in criminal and civil liability. E-Plan will investigate incidents involving such violations. If criminal activity is suspected, E-Plan may involve and will cooperate with law enforcement, as necessary. Examples of system or network security violations include, but are not limited to, the following:

- Unauthorized access to or use of data, systems or networks, including any attempt to probe, to scan, or to test the vulnerability of a system or network, or to breach security or authentication measures without express authorization or invitation of E-Plan.
- Unauthorized monitoring of data or traffic on any network or system without the express authorization of E-Plan.
- Interference with service to any user, host, or network, including, without limitation, mail bombing, flooding, deliberate attempts to overload a system, and broadcast attacks.
- Forging of any TCP-IP packet header or any part of the header information in an electronic mail (email) or traditional mail package.
- Sharing of User ID's and Passwords is strictly prohibited.



**Email**

Accept

Sending unsolicited mail messages, including, without limitation, commercial advertising and informational announcements, is explicitly prohibited. The email accounts for the E-Plan Emergency Response Information System are intended solely for system business; therefore, correspondence that does not concern E-Plan issues is prohibited.

**Sensitive Material**

Accept

The E-Plan Emergency Response Information System is a secure, non-public information source on the web. The data may include sensitive and proprietary information. As such, only individuals issued accounts by an Authorized Authority or E-Plan will have access to the system. Therefore, any unauthorized use or distribution of either E-Plan User accounts or E-Plan material(s) may result in criminal or civil liability.

**Reporting Violations**

Accept

E-Plan requires that anyone who believes that

- 1) there has been a violation of this Acceptable Use Policy or
- 2) unauthorized personnel have used, are using, or plan to use the E-Plan Emergency Response Information System to contact the E-Plan Administrator by calling telephone number (972) 883-2631 or sending an email to [eplan@utdallas.edu](mailto:eplan@utdallas.edu).

If available, please provide the following information:

- The identity of the person or persons responsible for committing the alleged violation
- The date and time of the alleged violation
- Evidence of the alleged violation

E-Plan may take any one or more of the following actions in response to complaints:

- Issue warnings: written or oral
- Suspend the User's account
- Terminate the User's account
- Bring legal action to enjoin violations and/or to collect damages, if any, caused by violations

Please sign and date below to indicate that you have read, understand, and agree to abide by the Terms and Conditions outlined above in the Acceptable Use Policy.

User:

Name: \_\_\_\_\_  
(Printed)

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

## Glossary – Abbreviations and Acronyms

<b>128-bit SSL</b>	128-bit Secure Sockets Layer
<b>CGI</b>	Common Gateway Interface
<b>CHRIS</b>	Chemical Hazards Response Information System
<b>CSEPI</b>	CyberSecurity and Emergency Preparedness Institute
<b>ECS</b>	Erik Jonsson School of Engineering and Computer Science
<b>DHS</b>	Department of Homeland Security
<b>EPA</b>	Environmental Protection Agency
<b>EPCRA</b>	Emergency Planning and Community Right-to-Know Act
<b>HazMat</b>	Hazardous Material
<b>HVAC</b>	Heating, Ventilating and Air Conditioning
<b>IEC</b>	International Electrotechnical Commission
<b>IKS</b>	INTELLIKEY System
<b>ISO</b>	International Organization for Standardization
<b>MSDS</b>	Material Safety Data Sheets
<b>LEPC</b>	Local Emergency Planning Committee
<b>RMP</b>	Risk Management Plan
<b>SERC</b>	State Emergency Response Commission
<b>SMS</b>	Short Message Service
<b>SSL</b>	Secure Sockets Layer
<b>UPS</b>	Uninterruptible Power Supply
<b>UT Dallas</b>	University of Texas at Dallas

LINDA LINGLE  
GOVERNOR

MAJOR GENERAL ROBERT G. F. LEE  
DIRECTOR OF CIVIL DEFENSE

EDWARD T. TEIXEIRA  
VICE DIRECTOR OF CIVIL DEFENSE




PHONE (808) 733-4300  
FAX (808) 733-4287

**STATE OF HAWAII**  
**DEPARTMENT OF DEFENSE**  
**OFFICE OF THE DIRECTOR OF CIVIL DEFENSE**  
3949 DIAMOND HEAD ROAD  
HONOLULU, HAWAII 96816-4495

December 15, 2009

TO: Mr. Laurence K. Lau, Chair  
Hawaii State Emergency Response Commission

FROM: Edward T. Teixeira   
Vice Director of Civil Defense

SUBJECT: HSERC Meeting – December 17, 2009

I am unable to attend the December 17, 2009, HSERC meeting due to a conflicting schedule.

I hereby appoint Clarice Chung from State Civil Defense to represent me at the above meeting with all the rights as a voting member.