The University of Texas at Dallas (UT Dallas)
Erik Jonsson School of Engineering & Computer Science
CyberSecurity and Emergency Preparedness Institute (CSEPI)

When every second counts ...

E-Plan Implementation Guide for Federal, State, and Local Authorizing Authority

Document Change History

Revision	Details of Revision	Date
1.0	Initial release	8/1/2008
2.0	Add Appendix A – Acceptable Use Policy	6/14/2010

Table of Contents

Glossary

This Glossary contains a list of abbreviations and acronyms followed by definitions of terms.

ABBREVIATIONS and ACRONYMS	
DHS	Department of Homeland Security
EPA	Environmental Protection Agency
EPCRA	Emergency Planning and Community Right to Know Act
Hazmat	Hazardous Material
LEPC	Local Emergency Planning Committee
RMP	Risk Management Plan
SERC	State Emergency Response Commission
UT Dallas	The University of Texas at Dallas

1. Introduction

E-Plan was developed through a cooperative agreement between EPA Region 6, the Texas Council on Environmental Quality, and The University of Texas at Dallas (UT Dallas) in 2000. In the last ten years, E-Plan has grown from a prototype, beta tested in Corpus Christi, Texas, to the nation's largest internet accessible database of fixed facility chemical hazards, and is designed specifically for use by the emergency management community. E-Plan is designed specifically to accommodate that group, with extremely easy to understand web-interfaces, navigation features, and search utilities. 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.

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's 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).

2. 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.

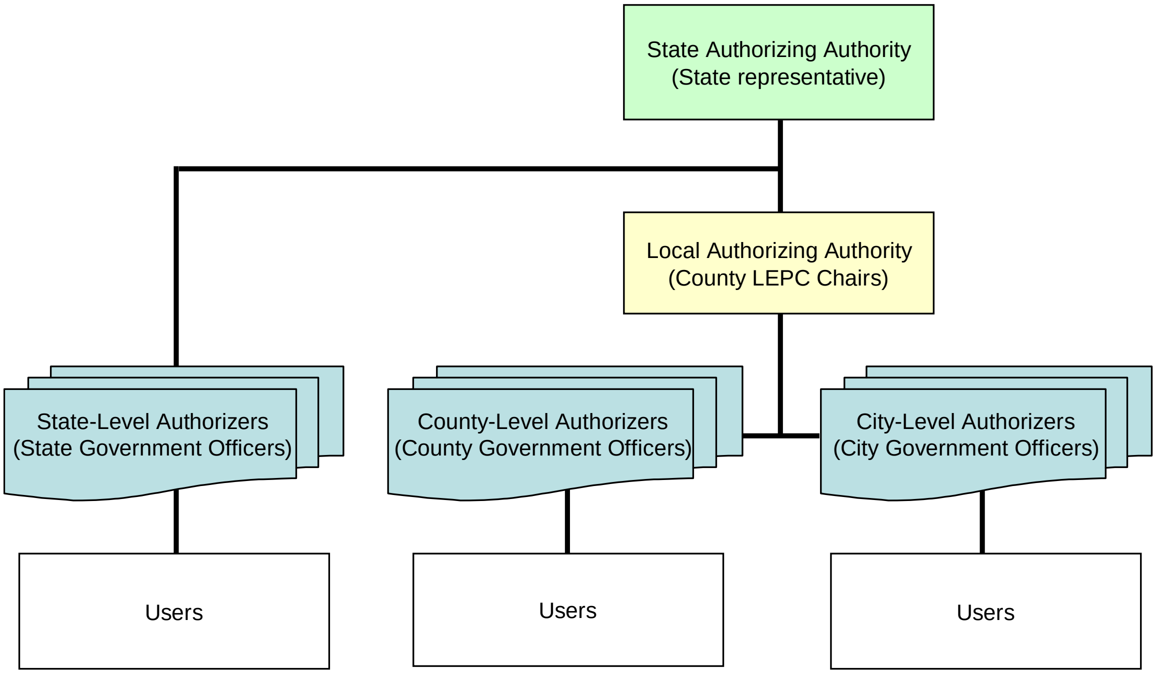
State Authorizing Authority
(State representative)
Local Authorizing Authority
(County LEPC Chairs)
State-Level Authorizers
(State Government Officers)
County-Level Authorizers
(County Government Officers)
City-Level Authorizers
(City Government Officers)
Users
Users
Users

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

2.1 Appointing State Representative

Once a State has determined 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.

2.2 Approving State-Level Authorizers

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

2.3 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 the State representative approves a LEPC Chair for a county, the LEPC Chair will approve the Authorizers for their county.

Once an LEPC within a state has determined 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 allowed 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

3. Federal Authorizing Authority Hierarchy

Once a Federal agency has determined 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 leaders in decision making on behalf of their respective agency to respond to agency-specific requests (users) to access E-Plan.

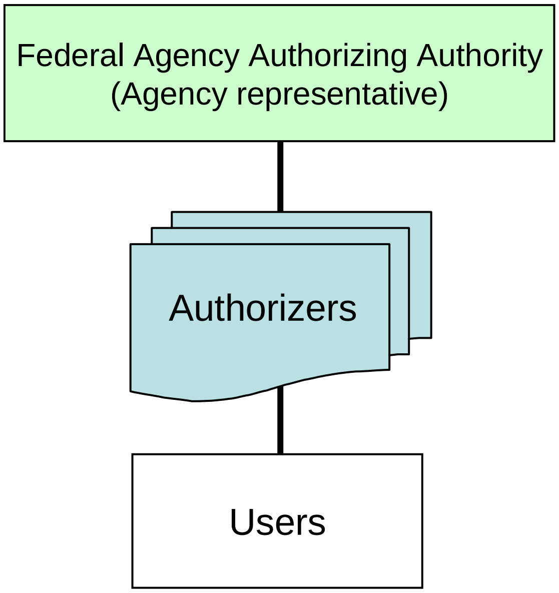

Figure 2 – E-Plan for Federal Authorizing Authority Hierarchy

4. E-Plan Account Request and Approval Process

4.1 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. They must complete the entire form including
   a. Read, understand, and fill in the "E-Plan Acceptable Use Policy" form (see Appendix A)
   b. Identify and select their authorizer from the E-Plan Authorizing Authority list

2. Upon receipt of the completed "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".

4.2 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 users must complete and submit the online "User Account Request" form on the E-Plan home page at https://erplan.net. They must complete the entire form including
   a. Read, understand, and fill in the "E-Plan Acceptable Use Policy" form (see Appendix A)
   b. Identify and select their local authorizer from the E-Plan Authorizing Authority list

2. Upon receipt of the completed "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 A – E-Plan Acceptable Use Policy

To E-Plan Account Requestor:

This 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 System). E-Plan reserves the right to modify the Acceptable Use Policy at any time and without notice. You must read, understand, and abide by the Terms and Conditions as set forth below. By checking the boxes below, you agree to the Acceptable Use Policy.

□ **Illegal Action**

The E-Plan 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**

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 Names and Passwords is strictly prohibited.

□ **Email**

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

□ **Sensitive Material**

The E-Plan 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 E-Plan will have access to the system. Therefore, any unauthorized use or distribution of either E-Plan accounts or E-Plan material(s) may result in criminal or civil liability.

□ **Reporting Violations**

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 System to contact the E-Plan Administrator by calling telephone number (972) 883-2631 or sending an email to 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 enter your full name 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.

E-Plan Account Requestor

Full Name: Date: (mm/dd/yyyy)