Overview

The Environmental Screening Tool (EST) is a secure Internet application accessed via a web browser. It supports the Florida Department of Transportation (FDOT) and Metropolitan Planning Organizations/Transportation Planning Organizations (MPOs/TPOs) in the environmental review process for transportation projects. The Office of Environmental Management (OEM) grants access to specific named users based on access approval by the FDOT Efficient Transportation Decision Making (ETDM) Coordinators.

The Area of Interest (AOI) Tool within the EST Map Viewer allows a user to define and analyze an area anywhere in Florida to learn more about people, places, and natural resources at that location. The AOI is primarily used by FDOT and MPO/TPO project teams to gain a preliminary understanding of a project area. It may also be used by local governments to support their transportation project delivery.

How Local Governments Request Accounts

To request AOI accounts, the local government should:

1. Coordinate internally to identify one person and a backup within their agency who need access to the AOI Tool.
2. Contact the appropriate FDOT ETDM Coordinator assigned to the FDOT District where the agency jurisdiction is located. A map of the FDOT Districts and corresponding FDOT ETDM Coordinator contact information is located the ETDM Contacts Page.
3. Provide the following information via email to the FDOT ETDM Coordinator for each user:
    - Name
    - Title
    - Organization
    - Address
    - Phone Number
    - Email Address

Upon authorization, the FDOT ETDM Coordinator forwards the request to the OEM Help Desk to set up the account. When the account is set up, the user receives an email with instructions to get started.

The local government representative is responsible for promptly informing the FDOT ETDM Coordinator when access is no longer needed, or the user is no longer employed by the agency.

Rules for Acceptable Use

It is the policy of the Florida Department of Transportation (FDOT) to treat information and information technology resources as strategic assets. As such, these assets must be protected from misuse, abuse and loss through the management of a comprehensive information technology resources

security program. Authorized users of the EST and AOI Tool are responsible for adhering to the following personnel security requirements:

1. Each individual with authenticated access to the EST is required to adhere to these procedures and all information security standards and procedures of FDOT.
2. Each individual with authorized access to the EST is expected to protect confidential information available on the site such as the locations of archeological sites, and threatened and endangered species. Precise locations of these resources are sensitive. Unauthorized distribution of the data may lead to vandalism and destruction of the resources. In particular, archaeological site location information is exempt from Florida's public records laws under Florida Statute 267.135 and may be withheld when the Division of Historical Resources finds that its release could create a risk of site damage. Do not publish, distribute, post on the internet or otherwise disseminate data which would reveal archaeological site locations. Refer requests for the data to the Division of Historical Resources.
3. Each individual accessing the EST is expected to use good judgment and common sense in the workplace to avoid abuse and inappropriate use of resources. It is inappropriate to use any resource in a way that will: interfere with the timely performance of an individual's normal work duties; reduce public confidence; support a personal business; support political or religious activities; or detract from routine work functions. Furthermore, it is inappropriate for personnel to access, send, store, create, or display sensitive materials, including but not limited to, gambling, any illegal activity, sexually explicit materials, or materials that include profane, obscene, or inappropriate language, or discriminatory racial or ethnic content. Such activities will be considered misuse or abuse of information technology resources.
4. Each individual with authorized access to the EST shall be held responsible for systems security to the degree that his or her job requires the use of information and associated systems. All personnel are responsible for using information technology resources only for the purpose intended, complying with all controls established by information technology resource owners and custodians, protecting sensitive information against unauthorized disclosure, and protecting FDOT from unauthorized access to information resources, including physical connections to the FDOT network.
5. Each individual that has been granted privileged or specialized security authorizations will be considered to be in a position with trusted security requirements. This includes, but is not limited to, individuals that grant security authorizations, administer networks and servers, use voice and telecommunications diagnostic equipment, use remote control software, migrate software and code from test to production environments, or perform other security-related activities deemed sensitive or critical by their manager or supervisor.
6. All users are required to immediately report any violations of this procedure, including unlawful accesses, suspected intrusions, and other information resource security incidents, including theft, to the EST Application Owner via help@fla-etat.org.