eProject eXpress Security

LBNL has extensive experience protecting business-sensitive information provided by contractors and their customers. From the very beginning, the eProject Builder system and eProject eXpress pathway were designed to protect users' information using state-of-the-art security features including: encrypted communication protocols, two-step user authentication, and regular—as well as randomly occurring—vulnerability testing and remediation.

Encrypted communication protocol

- Communication protocol encrypted by Transport Layer Security (i.e., https)

Two-step user authentication

- Two-step authentication required with every session log-in—similar to high-security e-commerce websites
- Users enter password and then access and enter randomly generated authentication code

Restricted access

- Each project is accessible by only one customer and one contractor contact
- Additional users may be granted read-only access to approved projects
- Data held in secure national lab servers

Vulnerability testing and remediation

- Two levels of regular security scans:
  1. LBNL IT department security scans
  2. Third-party government cyber security expert scans
- ePB has achieved and maintains a total *Rapid 7 Nexpose* risk score of zero

Security expert testimonial

"Through the remediation efforts by the [LBNL] team, the total [Rapid 7 Nexpose] risk score was driven to 0 (zero) by May of 2015 and has remained at 0… With the regular aggressive scanning and fast remediation efforts by LBNL, I am confident in the security of the [ePB] web applications at LBNL."

Paul Henry
CEO *v*Net Security, LLC

Contact and technical support
epb-support@lbl.gov
510-486-7442