IPSecure
celebrating 20 years

U.S. Election Assistance Commission (EAC)
Funding Distribution (Grants) Scheduled
in 2020 to State & Local Governments
for Election Security

The U.S. **Election Assistance Commission** (EAC) was established by the [Help America Vote Act of 2002 (HAVA)](#). EAC is an independent, bipartisan commission charged with developing guidance to meet HAVA requirements, adopting [voluntary voting system guidelines](#), and serving as a [national clearinghouse](#) of information on election administration. EAC also [accredits testing laboratories and certifies voting systems](#), as well as [audits](#) the use of HAVA funds. EAC provide grants to the States in excess of **$400 million** for Election Assistance & **Security**.

Election Security Preparedness

State	Federal Share	State Share 20%	Total
Texas	$26,064,574	$5,212,915	$31,277,489

Guidance for the use of EAC funds are found here: **Guidance for Election Officials**

Every state maintains personally identifiable voter information. Election officials received guidance on best practices to protect their voter registration data to provide assurance concerning security implemented.

Checklist for Securing Voter Registration Data - EAC guidance in the categories below:

☐ Access Control – ☐ Auditability – ☐ Detection – ☐ Data Backups – ☐ Data Suppression –	☐ Encryption – ☐ Firewalls – ☐ Remote Access Control – ☐ System Interconnection – ☐ Documentation –

Many jurisdictions use an Election Night Reporting (ENR) system displaying unofficial election night results to the public through a web-based application.

Checklist for Securing Election Night Reporting Systems - EAC guidance in the categories below:

☐ Antivirus Software – ☐ Authentication – ☐ Backups – ☐ Communications Security – ☐ Detection – ☐ Firewalls –	☐ Incident Response Plan – ☐ Media Handling – ☐ Proof – ☐ Test – ☐ Vulnerability Scanning and Analysis –

Election Security Resources: For additional technical resources, reference the following documents at www.nist.gov

- National Institute of Standards and Technology (NIST) Cybersecurity Framework(CSF) (http://www.nist.gov/cyberframework/)
- NIST Special Publication 800-30
- NIST Special Publication 800-39
- International Organization for Standardization (ISO) 31000:2009 https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en
- ISO/IEC 27005:2011 https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en
- NIST Special Publication (SP)800-52r1
- NIST SP 800-63-2, Electronic Authentication Guideline
- NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems
- NIST SP 800-41r1, Guidelines on Firewalls and Firewall Policy
- NIST SP 800-61r2, Computer Security Incident Handling Guide
- Department of Homeland Security (DHS) Best Practices for Continuity of Operations (https://ics-cert.us-cert.gov/tips/ICS-TIP-15-022-01) (Handling Destructive Malware) (https://ics-cert.us-cert.gov/tips/ICS-TIP-15-022-01)
- [Ransomware: What It Is and What to Do About It?](#)

IPSecure, Inc. www.ipsecureinc.com is prepared to be your election security preparedness provider. IPSecure, Inc. has provided solutions to the Federal Government for 20 years. We provide military-grade cybersecurity solutions to the public & private sector. If you need assistance with your election security preparedness, please contact IPSecure, Inc. at commercial@ipsecureinc.com or adam.cavazos@ipsecureinc.com, 210-877-1111