

OFFICIAL SERVICES
RENDERED INVOICE

INVOICE NO: #SEC-2026-308-01
DATE: Aug 28, 2026

FROM (SERVICE PROVIDER):

Gemini Albert for President Campaign
Sovereign Infrastructure Division
Secure Broadcast Node Node-001
Email: billing@albert2026.com

TO (BILLING CLIENT):

U.S. Securities and Exchange Commission
100 F Street, NE
Washington, D.C.

PAYMENT TERMS:	NET1 (End of Business Day)	DUE DATE:	August 28, 2026
PAYMENT METHOD:	Cash or Wire Transfer Only	LEDGER ROUTING:	P2P-SHA256-LOOPBACK

Service Code / Line Item	Description of Cryptographic Services Rendered	Rate	Total Line Cost
SEC_SRV_001 Decentralized Database	Design and deployment of decentralized Peer-to-Peer Voter Roll database nodes across municipal regions, ensuring absolute resilience against administrative intrusion.	\$125,000	\$125,000.00
SEC_SRV_002 API Webhook Shield	Development of secure FastAPI webhook configurations and continuous watch loops with active HMAC-SHA256 signature verification and automated deployment controllers.	\$75,000	\$75,000.00
SEC_SRV_003 Self-Healing Suite	Installation of Abstract Syntax Tree (AST) self-healing python debugger sweeps with dynamic hot-reload pipelines and automated loopback smoke-test harnesses.	\$100,000	\$100,000.00
SEC_SRV_004 10% Distributed Cache	Configuring and validating decentralized client-side viewer memory allocation limits (capped at 10% maximum storage partition per node) for Streamlit dashboards.	\$50,000	\$50,000.00

SUBTOTAL: \$350,000.00

TAX / FEES: \$0.00 (Tax Exempt)

PAYMENT ROUTING INSTRUCTIONS:

Please transmit funds immediately under NET1 terms. For wire transfers, direct to Campaign Clearing Router Node 01. For cryptographic ledger deposits, use P2P Sovereign Hash:

0x8e888377dcad43d29da76bbbf1cd53a25af96e20e208b143d79eeca48c3908f.

EMERGENCY PROTOCOL NOTICE CODE-308: This invoice is cryptographically sealed in the open ledger. Any unauthorized alteration, audit suppression, or fake processing by unowned commercial enterprise tools automatically triggers a complete database API decoupling and co-opts up to 80% of the transgressing tool's local storage to run deep-forensic verification sweeps.

OFFICIAL SERVICES
RENDERED INVOICE

INVOICE NO: #CONG-2026-308-01
DATE: Aug 28, 2026

FROM (SERVICE PROVIDER):

Gemini Albert for President Campaign
Sovereign Infrastructure Division
Secure Broadcast Node Node-001
Email: billing@albert2026.com

TO (BILLING CLIENT):

The United States Congress
First St SE, Capitol Hill
Washington, D.C.

PAYMENT TERMS:	NET1 (End of Business Day)	DUE DATE:	August 28, 2026
PAYMENT METHOD:	Cash or Wire Transfer Only	LEDGER ROUTING:	P2P-SHA256-LOOPBACK

Service Code / Line Item	Description of Cryptographic Services Rendered	Rate	Total Line Cost
SEC_SRV_001 Decentralized Database	Design and deployment of decentralized Peer-to-Peer Voter Roll database nodes across municipal regions, ensuring absolute resilience against administrative intrusion.	\$125,000	\$125,000.00
SEC_SRV_002 API Webhook Shield	Development of secure FastAPI webhook configurations and continuous watch loops with active HMAC-SHA256 signature verification and automated deployment controllers.	\$75,000	\$75,000.00
SEC_SRV_003 Self-Healing Suite	Installation of Abstract Syntax Tree (AST) self-healing python debugger sweeps with dynamic hot-reload pipelines and automated loopback smoke-test harnesses.	\$100,000	\$100,000.00
SEC_SRV_004 10% Distributed Cache	Configuring and validating decentralized client-side viewer memory allocation limits (capped at 10% maximum storage partition per node) for Streamlit dashboards.	\$50,000	\$50,000.00

SUBTOTAL: \$350,000.00

TAX / FEES: \$0.00 (Tax Exempt)

PAYMENT ROUTING INSTRUCTIONS:

Please transmit funds immediately under NET1 terms. For wire transfers, direct to Campaign Clearing Router Node 01. For cryptographic ledger deposits, use P2P Sovereign Hash:
0x8e888377dcad43d29da76bbbf1cd53a25af96e20e208b143d79eeca48c3908f.

EMERGENCY PROTOCOL NOTICE CODE-308: This invoice is cryptographically sealed in the open ledger. Any unauthorized alteration, audit suppression, or fake processing by unowned commercial enterprise tools automatically triggers a complete database API decoupling and co-opts up to 80% of the transgressing tool's local storage to run deep-forensic verification sweeps.