

Response to RFP No. 2026-DHS-0042

Cybersecurity Awareness Training Services

Issued By: Department of Homeland Security (Sample)

Submitted By: IssuraDoc Solutions LLC (Sample)

DUNS: 12-345-6789 | CAGE: AB1C2

Date of Submission: July 15, 2026

Point of Contact: Jane Doe, BD Director — jane.doe@sample.com

SAMPLE — FOR ILLUSTRATION PURPOSES ONLY — IssuraDoc

Solicitation No.	RFP-2026-DHS-0042
NAICS Code	611430 — Professional and Management Development Training
Set-Aside	Small Business (SB)
Contract Type	Firm Fixed Price (FFP)
Period of Performance	12 months with two (2) one-year options

Section 1 — Executive Summary

IssuraDoc Solutions LLC (hereinafter "Offeror") is pleased to submit this proposal in response to Request for Proposal No. 2026-DHS-0042 for Cybersecurity Awareness Training Services. We offer a proven, scalable training solution designed to meet the Department's requirements while delivering measurable improvements in employee security posture across the enterprise.

Our approach combines instructor-led virtual training, on-demand eLearning modules, and quarterly phishing simulation exercises — all tailored to the DHS operating environment and compliant with NIST SP 800-50 and FISMA requirements.

We are confident that our solution, pricing, and team represent the best value to the Government.

Section 2 — Technical Approach

2.1 Program Overview

The Offeror proposes a three-tier training architecture that addresses awareness at the individual contributor, manager, and executive levels. Each tier includes distinct learning objectives, delivery modalities, and assessment benchmarks aligned to the solicitation's Performance Work Statement (PWS).

2.2 Curriculum Design

- Modules aligned to NIST Cybersecurity Framework (CSF) core functions: Identify, Protect, Detect, Respond, Recover
- Role-based training paths for general staff, privileged users, and system administrators
- Quarterly content refresh cycle to address emerging threats and updated agency requirements
- 508-compliant content delivery accessible to all personnel

2.3 Delivery Methodology

Training will be delivered through a Government-approved Learning Management System (LMS) integrated with the agency's existing SSO infrastructure. Instructor-led sessions (ILT) will be conducted virtually via approved video conferencing platforms and recorded for asynchronous access.

SAMPLE — FOR ILLUSTRATION PURPOSES ONLY — IssuraDoc

Section 3 — Past Performance

The Offeror has successfully delivered cybersecurity awareness programs to three Federal civilian agencies over the past four years. Representative examples include:

Agency	Contract Value	Period	Outcome
Dept. of Commerce (Sample)	\$1.2M / year	2023–2025	94% completion rate; phishing click-through reduced by 61%
GSA (Sample)	\$780K / year	2024–2026	FISMA audit: All awareness metrics rated Effective
Dept. of Energy (Sample)	\$950K / year	2022–2024	Zero reportable incidents attributed to user error post-training

Section 4 — Management Approach

The Offeror will assign a dedicated Program Manager (PM) as the single point of contact for the Contracting Officer's Representative (COR). The PM will maintain a project management plan updated monthly and conduct bi-weekly status calls with agency stakeholders.

- Monthly progress reports delivered by the 5th business day of each month
- Issue tracking via Government-approved project management platform
- All deliverables submitted for Government review with a minimum 5-business-day review window

Section 5 — Price Summary

Pricing is submitted under separate cover per solicitation instructions. The Offeror confirms that all prices are Firm Fixed Price and inclusive of all labor, materials, overhead, and profit.