U.S. DEPARTMENT OF HOMELAND SECURITY (DHS)
Cybersecurity and Infrastructure Security Agency (CISA)
Emergency Communications Division (ECD)

STATEMENT OF REQUIREMENTS (SOR)
National Cyber-Forensics and Training Alliance Annual Membership

1.0 GENERAL

1.1. Background

CISA ECD's mission is to advance emergency communications in partnership with Public Safety and National Security/Emergency Preparedness communities. ECD does this to achieve an end-state where interoperable, secure, and resilient emergency communications enable daily operations and incident response throughout the nation, without disruption from any hazard or threat. Specifically, ECD works to protect infrastructure and emergency communications capabilities across all levels of government in two critical infrastructure sectors: The Emergency Services Sector and The Communications Sector. ECD also works to ensure the following National Critical Functions are reliably sustained and made as resilient as possible: Provide Public Safety; Provide Medical Care; Prepare for and Manage Emergencies; Operate Government; Enforce Law; Provide Wireless Access Network Services; Provide Wireline Access Network Services; and Operate Core Network.

Threat-investigation capabilities currently available to CISA do not target the public safety, national security/emergency preparedness communications domain and are not likely to do so because of the intelligence community's focus on threats facing other critical infrastructure sectors.

Today, more public safety functions rely on Internet Protocol (IP)-based communications for data, voice, video, and other IT services and for their communications with the public. As commercial telecommunications companies migrate technologically to IP networks, there is a convergence of IP-based communications used by public safety, especially in the 9-1-1 ecosystem, with telecommunications company-supported communications. Concurrently, the Public has come to expect that their SLTT emergency services functions will leverage the same IP-based technologies that they use every day. These convergences and increased reliance on IP-hosted technologies expose public safety and commercial telecommunications companies to both physical and cyber-attack vectors not previously considered or anticipated. By establishing a reliable threat information flow from NCFTA to CISA, CISA can better prepare SLTT jurisdictions and the MISPs they rely on to better protect their critical emergency communications systems from the rapidly evolving threat environment.

1.2. Scope

This SOR provides CISA ECD with an annual National Cyber-Forensics & Training Alliance (NCFTA) membership. The membership will provide mission related threat information services to improve ECD's awareness of and quantify the severity of threats facing public safety, and national security/emergency preparedness emergency communications stakeholders through NCFTA's Remote Partnership model.

2.0 Specific Requirements

The Remote Partnership includes the following:

- NCFTA Listservs (Supported by full-time intel analysts)
- Custom Intelligence Reports (Soft limit of 10 per year)
- Other Intel Products (link charts, shared intelligence)
- Virtual Intel Analyst Direct Support
- Receive NCFTA malware feeds and file analysis support
- Access to NCFTA data, network, and tools – upon request through NCFTA POC – included in annual membership fee
- Keyword monitoring (Multi-Platform)
- Attendance at NCFTA conference "DISRUPTION" (limit of 5)
- Reduced fees for additional attendance at NCFTA Cyber Crime Forum (50% off)
- Reduced fees to attend NCFTA sponsored training
- Virtual participation in cross-industry working groups
- Participation in on-site Analyst Workshops when scheduled in advance
- Internet Fraud Alert (organizational subscription)
- Access for on-site visits to Pittsburgh and New York offices to work on cases (periodic visitor status)

3.0 Period of Performance

The period of performance for this requirement shall be for a base period of 12 months and four (4) 12-month option periods.

4.0. Invoices and Payment Provisions

Invoices shall be prepared per FAR Clause 52.212-4. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

1) Cover sheet identifying DHS/CISA/ECD;
2) Order Number;
3) Modification Number, if any;
4) UEI Number;
5) Month services provided;
6) Contract Line Item Number (CLIN) and Accounting Classifications;
7) CLIN and description for each billed item.
8) Any additional supporting information as required by this contract.
9) ATTN: CISA/ECD

The contractor shall submit invoices monthly. The Contractor shall submit the invoice electronically to the address below:

E-mail: [redacted]

Simultaneously the Contractor shall provide an electronic copy of the invoice to the following individuals:

E-mail: [redacted]

Additionally, the contractor shall prepare and submit a sufficient and procurement regulatory compliant invoice and receiving report for technical certification of inspection/acceptance of services and approval for payment. The contractor shall attach supporting information to the invoices and receiving reports substantiating all costs for services performed. The receiving agency's written or electronic acceptance by the COR and date of acceptance shall be included as part of the supporting documentation. If the invoice is submitted without all required supporting documentation, the invoice shall be rejected. The Government reserves the right to have all invoices and supporting documentation reviewed by the Contracting Officer prior to payment approval.