Non-Intrusive Inspection Integration (NII-I)

Anomaly Detection Algorithm Statement of Work (SOW)

April 14, 2023

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

Department of Homeland Security Customs & Border Protection (CBP) Statement of Work (SOW) for Non-Intrusive Inspection (NII) Anomaly Detection Algorithm (ADA)

1.0 BACKGROUND

The Non-Intrusive Inspection (NII) Systems Program exists within the Customs and Border Protection (CBP) Office of Field Operations (OFO) with the mission to develop, acquire, deploy, operate, and maintain a wide variety of NII technology detection systems which support operations in all CBP operational vectors. NII technology is currently deployed to airport, seaport, international mail, express consignment, rail, and commercial truck / private vehicle / pedestrian land border port of entry (POE) operational environments. NII systems such as vehicle X-ray, radiation portal monitors (RPM), chemical detectors, etc., are tools that provide a more efficient and effective means to screen conveyances and individuals for contraband and identify threats, compared to manual search techniques.

The NII Systems Program is working to recapitalize on existing assets and expand coverage of NII scanning technology with modern, integrated Commercial Off-the-Shelf (COTS) systems capable of greatly increasing scanning throughput. A key goal of the program is to reduce the current NII examination processing time to: (1) increase the number of cargo conveyances, private vehicles, packages, containers, and individuals scanned, (2) to improve security, and (3) reduce the number of officer / agent hours used to conduct NII examinations – both without impact to the flow of legitimate trade and travel. In recent years, the NII Program has begun executing a limited number of technology demonstrations (TD) involving Multi-Energy Portal (MEP), Low-Energy Portal (LEP), and CT mail-scanning X-ray systems with the intent to pursue full NII integration across a wide range of CBP systems, while implementing a variety of innovative concepts of operation (CONOP) to improve operational efficiencies, eliminate administrative redundancies, increase CBP officer (CBPO) productivity, and further enhance CBPO safety.

2.0 SCOPE

The development and implementation of Anomaly Detection Algorithms (ADA) to assist CBP officers' image analysis is a key component of the above-mentioned demonstrations, with specific interest on algorithms which facilitate screening for contraband and anomaly detection in passenger vehicles and cargo conveyances. These TD system deployments are already generating a large volume of commerce image data streams, which is being compiled in the CBP cloud environment and made available for various analyses including algorithm development.

Anomaly detection algorithms delivered under this SOW must increase the ability to inspect a conveyance thoroughly with little to no impact to traffic flow, have a high true positive rate of identifying suspected anomalies with positive confirmation of the anomaly and/or a high true negative rate resulting in identifying "clean" conveyances. The ideal is to build algorithms that can detect anomalies of the entire vehicle; however, CBP understands an ensemble of ADAs may be necessary to meet all CBP's requirements.

When delivering an ADA, use case descriptions are required and must include, with justification, which component(s) of the vehicle or contraband detection the algorithm performs the best on, (i.e., identification of the specific areas of the conveyance, what characteristics of the contraband, or anomalies, and modification location).

The high-level use cases of interest to CBP include, but are not limited to:

- Commercial Operated Vehicles (COV) to include cargo and cab
  - Anomalies in both homogeneous and heterogeneous loads
  - Conveyance modifications in both homogeneous and heterogeneous loads
  - Manifest verification based on Harmonized Tariff Schedule
  - Specific item categories in both homogeneous and heterogeneous loads
- Privately Owned Vehicles (POV)
  - Anomalies detected in full vehicle body
  - Conveyance modification
  - Specific item categories

The desired end state for the NII Systems Program is an open-source platform that supports autonomous image analysis for low-risk trade and travel, provides assistance to CBP officers for review of high-risk trade and travel images, and the analysis of more complex images. Therefore, it is critical that all algorithms can be integrated easily into the larger NII platform and not solely be integrated into closed proprietary applications/systems. ADA should increase the thoroughness and/or reduce the time needed overall to conduct image review, to clear low-risk shipments, and to reduce CBP officer manpower commitments to sustain high volume NII scanning operations.

In this solicitation, CBP defines the term algorithm to include the AI model and any supporting software which enables the models' use (e.g., inference input, inference output, explanations, and other metrics).

3.0 PERIOD OF PERFORMANCE

The contract period of performance is intended to be one base year and 4 option years for each awarded contract.

4.0 PLACE OF PERFORMANCE

The primary location of the place of performance for CBP Office of Field Operations (OFO) is 1300 Pennsylvania Avenue NW Washington, DC 20004, and for CBP Office of Information Technology is Ashburn, VA. Contractors may also perform within their own facilities, for work that can be perform remotely. Remote work can be authorized based on individual Task/Solution requirements.

5.0 APPLICABLE DOCUMENTS

List of other applicable documents and industry standards:

- CBP Data Strategy
- DHS Directive 102-01
- DHS Directive 102-01-001
- CBP Security Policies and Procedures Handbook
- DHS/CBP Program Lifecycle Process Guide
- CBP OIT Agile Governance Framework
- DHS Systems Engineering Life Cycle (SELC)

- CBP SELC Process
- CBP SecDevOps Concept of Operations (CONOPS)
- Office of Accessible Systems and Technology (OAST) Compliance
- CBP Section 508 Directive Number 5510-040A
- DHS MD 4300A, DHS Sensitive Systems Policy and Directive, CBP Information Systems
- DHS Management Directive 140-01, Information Technology Security Program
- CBP Information Systems Security Policies and Procedures Handbook, HB 1400-05D
- All applicable National Institute of Standards and Technology (NIST) Special Publications (800 Series)
- DHS Enterprise Data Management Policy Directive 103-01
- CBP Technical Reference Model (TRM)
- CBP Enterprise Technical Architecture (ETA)
- CBP Directive, Infrastructure Services Division Product Testing
- Federal Data Center Consolidation Initiative FDCCI
- Passenger Systems Program Directorate (PSPD) Configuration Management Plan
- PSPD OIT Change Control Board Instructions
- PSPD Change Request Form Template
- Facilities Standard for Public Building Service PBS-100
- U.S. Land Port of Entry Design Guide Supplement
- National Information Exchange Model (NIEM)
- Business Process Modeling Notation
- ISO/IEC 11801:2002 2ND ED. 2002-09
- ISO 18000-6c GEN 2
- IEC 61156-5, -6

6.0 DELIVERY REQUIREMENT

No partial submissions are permitted unless specifically authorized at the time of award. Delivery of ADA solutions shall be made to CBP's designated algorithm mailbox. Each contract and each identified task under the contract will specify delivery locations for ADA solutions and products. Example locations include but are not limited to:

Delivery Address:

TBD at contract award

7.0 TYPE OF CONTRACT

This award will establish a Non-FAR Contract through the DHS Commercial Solution Opening Pilot Program (CSOP).

8.0 POINTS OF CONTACT

Contracting Officer: Joshua Bedregal Contract
Specialist: Peter Giambone Email:
peter.a.giambone@cbp.dhs.gov

9.0 DELIVERABLES AND SUPPORT

The scope shall include the following capabilities, which may be iteratively developed at the Task and Solutions level of the contract. All deliverables shall be delivered to the email address that will be provided after award.

a) Development and implementation of ADA Artificial Intelligence/Machine Learning (AI/ML) Solutions that provide automated identification of anomalies and/or norms, operator-assist to highlight regions of interest, identification of conveyance modifications, identification/verification of commodities, linkages to other CBP data sources, or some combination of these capabilities through a series of algorithms.
   1. Images will be provided by CBP for AI/ML training purposes.
   2. Development will utilize common data formats including but not limited to COCO file format and World Customs Organization (WCO) Unified File Format (UFF), within an open architecture and emphasize non-proprietary solutions suitable for various deployment architectures, including OEM NII systems, common integration platform / viewers and CBP Cloud environment, as well as aggregate solutions to combine results from multiple algorithms.
   3. Submissions must meet DHS cybersecurity regulations.

b) Services
   1. Expanded Feature Development (Product development features to support CBP operations). Government may require the contractors support in expanding CBP's ADA capability by helping it develop additional add on features or algorithm enhancement as the need arises.
   2. Support to enable model testing, evaluation, validation, and verification, to include automated metrics for continuous performance measurement.
   3. Implementation of an overall algorithm lifecycle to include MLOps (e.g., model refinement, re-training for model drift and data drift, bias, accuracy, performance monitoring).
   4. Support for continued model improvement to ensure that the solution is a continually learning and improving system which can adapt to adversarial adaptations.
   5. Travel to support deployment, training, and upgrades (NTE Amount)
      i. All contractor travel required by the Government will be reimbursed to the contractor in accordance with the Federal Travel Regulations (FTR). Local travel will not be reimbursed. The contract will include a NTE travel amount that cannot be exceeded without contract modification. The contractor exceeds this travel ceiling at its own risk.
      ii. The contractor shall be responsible for obtaining COR approval in writing at least 10 days prior to travel for all reimbursable travel in advance of each travel event.
      iii. Requests must identify:
         - The name of the traveler(s)
         - Destination(s) including itinerary
         - Purpose of the travel
         - Estimated cost breakdown (airfare, lodging, per diem, rental car, etc.)

c) Hardware
   1. Optional Hardware: The Government is not requiring hardware solutions; however, submitters may include hardware in their submissions as part of their

solutions.

Contract Data Requirements

TBD	TBD	TBD

10.0 COMPLIANCE REQUIREMENTS

10.1 Information Technology Security Compliance Requirements

The contractor shall adhere to all DHS and CBP IT security policies and the basic requirements, security authorization, encryption compliance, and pass security review.

10.1.1 DHS Security Policy Compliance Requirements

All hardware, software, and services provided under this CSOP contract must be compliant with DHS 4300A, the DHS Management Directive 140-01, and Information Security Program and CBP Information Systems Security Policies and Procedures Directive, HB 1400-05D.

10.1.2 Basic Requirements

The contractor shall adhere to all DHS and CBP IT security policies listed in the applicable documents section, including the guidelines and policies stated in the DHS Sensitive Systems Policy Directive 4300A or any subsequent, replacement or revised publication. This policy mandates DHS organizational elements, including contractors, follow guidelines outlined in the DHS MD 4300A, DHS Sensitive Systems Directive, Information Technology Security Program, Version 13, with attachments or any subsequent, replacement or revised publication.

DHS Directive 4300A, Basic Requirements outlines the management, operational and technical baseline security requirements (BLSR) for DHS Components to ensure confidentiality, integrity, availability, authenticity, and non-repudiation of sensitive information systems. The 4300A Directive provides greater detail of the BLSRs, including the roles and responsibilities associated with each.

CBP will provide personnel with the appropriate background investigation, clearance levels to support the security certification/accreditation processes under this Agreement in accordance with DHS MD 4300A, DHS Sensitive Systems Policy and Directive. During all systems development life cycle (SDLC) phases of CBP systems, CBP personnel will develop documentation and provide any required information for all levels of classification in support of the certification/accreditation process. In addition, all security certification/accreditation will be performed using the DHS certification/accreditation process, methodology and tools.
systems development life cycle (SDLC) phases of CBP systems, CBP personnel will develop documentation and provide any required information for all levels of classification in support of the certification/accreditation process. In addition, all security certification/accreditation will be performed using the DHS certification/accreditation process, methodology and tools.

Legacy air gapped non-integrated systems shall:

a) Wi-Fi shall not be used and be disabled.
b) All operating systems must use the requisite DHS Security Technical Implementation

Guides (STIGs) for hardening configurations.

c) All vendor contractors shall not remove image data from systems nor store said data on contractor networks.

d) Ground-truthing or tuning of systems will be performed only on CBP systems and not on contractor networks unless specifically authorized.

e) Integrated networked systems shall follow the above requirements and additionally:
   - If systems are using WIFI the design must be explicitly reviewed and approved by the CBP EIOD organization and Security and Technology Policy (STP).

f) Other wireless connectivity may be approved by EIOD

g) Systems must be patched and security updates maintained according to DHS patching standards (within 30 days usually) CBP Information Systems Security Policies and Procedures, Information Security Continuous Monitoring guidelines.

h) Username/Password authentication is not allowed.

10.1.3 Security Authorization

a) A Security Authorization of any infrastructure directly in support of the DHS information system shall be performed by the contractor as a general support system (GSS) prior to DHS occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization shall be performed in accordance with the DHS Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, Section 3, security categorization of the DHS information system.

b) At the beginning of the contract, and annually thereafter, the contractor shall provide the results of an independent assessment and verification of security controls in the contractor's format. The independent assessment and verification shall apply the same standards that DHS applies in the Security Authorization Process of its information systems. Any deficiencies noted during this assessment shall be provided to the Contracting Officer Representative (COR) for entry into the DHS Plan of Action and Milestone (POA&M) Management Process. The contractor shall use the DHS POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies shall be corrected within the timeframes dictated by the DHS POA&M Management Process. contractor procedures shall be subject to periodic, unannounced assessments by DHS officials. The physical aspects associated with contractor activities shall also be subject to such assessments.

c) On a periodic basis, the DHS and its components, including the DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the contractor under these clauses. Evaluation could include but is not limited to vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten working days' notice, at the request of the Government, the contractor shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS in the event of a security incident.

10.1.4 Encryption Compliance Requirement

a) Systems requiring encryption shall comply with FIPS 197 Advanced Encryption Standard (AES) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
b) Systems requiring encryption shall comply with National Security Agency (NSA) Type 2 or Type 1 encryption.
c) Only cryptographic modules that are FIPS 197 (AES 256) compliant and have received FIPS 140-2 validation at the level appropriate to their intended use may be used in systems requiring encryption.
d) Public Key Infrastructure (PKI) (see the Department of Homeland Security (DHS) Sensitive Systems Policy Directive 4300A).

10.1.5 Security Review

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The contractor shall afford DHS including the organization of the DHS Office of the Chief Information Officer, Office of Inspector General, the CBP Chief Information Security Officer, authorized COR, and other Government oversight organizations, access to the Contractor's and subcontractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. The contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of Government oversight organizations external to the DHS. The contractor shall provide access to the extent necessary for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS/CBP data or the function of computer systems operated on behalf of DHS/CBP, and to preserve evidence of computer crime.

10.1.6 Enterprise Security Architecture

The contractor shall utilize and adhere to the DHS Enterprise Security Architecture in accordance with applicable laws and DHS policies to the satisfaction of the DHS COR. Areas of consideration could include:

a) Use of multi-tier design (separating web, application, and data base) with policy enforcement between tiers
b) Compliance to DHS Identity Credential and Access Management (ICAM)
c) Security reporting to DHS central control points (i.e., the DHS Enterprise Security Operations Center (ESOC) and integration into DHS Security Incident Response
d) Integration into DHS Change Management (for example, the Infrastructure Change Control Board (ICCB) process)
e) Performance of security maintenance activities per continuous monitoring requirements

10.1.7 Information Assurance

Information Assurance (IA) is considered a requirement for all systems used to input, process, store, display, or transmit sensitive or national security information. IA is achieved through the acquisition and appropriate implementation of evaluated or validated commercial-off-the-shelf (COTS) IA and IA-enabled Information Technology (IT) products. These products provide for the availability of systems. The products also ensure the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions.

Strong preference is given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) that have been evaluated and validated by authorized commercial laboratories or by National Institute of Standards and Technology (NIST), as appropriate, in accordance with the following:

a) The NIST Federal Information Processing Standards (FIPS) validation program
b) The National Security Area (NSA) /NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program
c) The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement

10.1.8 Continuous Monitoring

The contractor shall participate in DHS Continuous Monitoring Strategy and methods or shall provide a Continuous Monitoring capability that the DHS determines acceptable. The DHS Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the contractor shall implement the following processes:

a) Asset Management
b) Vulnerability Management
c) Configuration Management
d) Malware Management
e) Log Integration
f) Security Information Event Management (SIEM) Integration
g) Patch Management

The contractor shall provide near-real-time security status information to the DHS ESOC. The contractor shall establish a monitoring scope at least as comprehensive and stringent as described in DHS 4300A Sensitive Systems Directive, “Incident Response.”

10.1.9 Specific Protections

Specific protections that shall be provided by the contractor include, but are not limited to the following:

a) Intrusion Detection Systems and Monitoring - The contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the Network Intrusion Detection System (NIDS) solution. The contractor is responsible for creating and maintaining the NIDS rule sets. The NIDS solution should provide real-time alerts. These alerts and other relevant information shall be located in a central repository. The NIDS shall operate 24x7x365. A summary of alerts shall be reported to the DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

b) Physical and Information Security and Monitoring - The contractor shall provide a facility using appropriate protective measures to provide for physical security. The facility will be located within the United States and its territories. The contractor shall maintain a process to control physical access to DHS IT assets. DHS IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS security office.

c) Vulnerability Assessments - The contractor shall provide all information from any managed device to DHS, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

d) Anti-malware (e.g., virus, spam) - The contractor shall design, implement, monitor and manage a comprehensive anti-malware service. The contractor shall provide all maintenance for the system providing the anti- malware capabilities to include configuration, definition updates, and comply with DHS' configuration management / release management requirements when changes are required. A summary of alerts shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

e) Patch Management - The contractor shall perform patch management services. The contractor shall push apply patches that are required by vendors and the DHS system owner. This is to ensure that the infrastructure and applications that directly support the DHS information system are current in their release and that all security patches are applied. The contractor shall be informed by DHS which patches are required by DHS through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS utilizes to fulfill their mission, shall be tested by DHS. However, the contractor shall be responsible for deploying patches as directed by DHS. It is recommended that all other applications (host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), Anti- malware, and Firewall shall be tested by the contractor prior to deployment in a test environment.

f) Log Retention - Log files for all infrastructure devices, physical access, and anti-malware should be retained online for 180 days and offline for three years.

10.1.10 Security Requirements for Unclassified Information Technology Resources

a) The contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

b) The contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(b.1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan in the Contractor's format, which shall be consistent with and further detail the approach contained in the officer's Quote. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(b.2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 USC 1441 et seq.),sections 5 and 6; the Federal Information Security Management Act (44 USC 3554 (b)) of 2014; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130, Appendix III, A.3.b (2).

(b.3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

c) Examples of tasks that require security provisions include -

(c.1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the Contractor's copy be corrupted; and

(c.2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract and certify that all non-public DHS information has been purged from any Contractor- owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

e) Within 6 months after contract award, the contractor shall submit written proof, in the Contractor's format, of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A, or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

10.1.11 Other Security Requirements

The contractor shall implement the minimum set of security requirements detailed below:

a) All systems processing CBP data shall use the CBP Desktop Management Group (DMG) Authorized Desktop Build (ADB) image.

b) All systems shall follow DHS/CBP requirements for Defense Information System Agency Security Technical Implementation Guide (DISA STIG) compliance.

c) All systems storing CBP data shall be encrypted using Bit Locker encryption or equivalent encryption approved by CBP Security.

d) All systems shall be capable of operating with CBP security applications and agents, such as Tenable Nessus, Tanium, Splunk, Digital Guardian, and Symantec Endpoint Protection.

e) All systems shall use TLS v1.2 or higher, encryption protocol when communicating over a network with internal and external systems and components.

f) All systems shall not use unauthorized programs and unsecure transfer protocols, such as ftp, telnet, http, and peer-to-peer networking.

g) All systems and network components shall be scanned for vulnerabilities at frequencies designated by CBP and PSPD, at 1-week, 2-week, or 1-month intervals. Based on the findings of the scan, the contractor shall remedy the vulnerability within 30 days.

h) All system and network component vulnerabilities shall be remediated within 30 days of discovery and documented in a plan of action and milestones (POA&M) if unresolvable within 30 days.

i) All systems shall have an adjudicated Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), Authority to Test (ATT) and/or Authority to Operate (ATO) for production deployment and operations.

j) All systems shall have an adjudicated and approved Interconnection Security Agreement (ISA) prior to establishing communications with and sending data to external entities.

k) All systems shall not store and maintain local copies of data (images, logs, messages) containing PII for longer than 7-days.

10.1.12 Management

a) Data cannot be viewed by non-US citizens or leave the United States boundary.

b) All contractors working with the data must be US citizens.

10.2 Technical Compliance Requirements

10.2.1 AI/ML Algorithm Requirements.

The contractor shall follow the below NII AI/ML ADA requirements.

10.2.1.1 Specific Algorithm Parameters

a) Design:

- **Unambiguous** – Algorithm should be clear and unambiguous –meaning that each step and their inputs/outputs should be clear and must lead to only one meaning.
- **Independent** – Algorithm should have step-by-step instructions and should be independent of any programming code or any other proprietary aspects that will limit the ability to be integrated into an open architecture.
- **Auditability** – Algorithm should not be black box and should include methods for explain-ability.

b) Output:

- **Usability** – Algorithm outputs should be usable with the ability to integrate into a variety of systems.
- **Anomaly Detection** – Output should be a file that draws bounding boxes around detected anomalies (e.g., Government preferred is COCO file format; however, this standard may be adjusted in the future to reflect the WCO UFF file format). No proprietary formats will be accepted.

- **Metrics** – Vendor should provide Classification Metrics (Confusion Matrix) (TN, TP, FN, FP) for all models. Examples of other metrics may include:
  - Intersection over Union (IoU)
  - Accuracy
  - AUC-ROC
  - F1 Score
  - Precision
  - Average Precision (AP)
  - Mean Average Precision (mAP)
- **Logs** – Vendor should provide all model training and validation logs generated during said processes.

10.2.1.2 Architecture/Integration Parameters

Must adhere to CBP Reference Architecture guidelines for all hardware specifications and required software. Any required software outside of CBP authorization, must go through the recommended CBP acquisition process, security testing, and vetting.

10.2.1.3 Data Requirements

a) Vendor shall use common data formats for inference and training (e.g., JSON, etc.).
b) Vendor will not use proprietary input/output data formats. Government preferred is COCO file format; however, this standard may be adjusted in the future to reflect the WCO UFF file format.
c) Vendor shall return all CBP data plus any derivate sets that were created (e.g., enriched, transformed, altered, aggregate, correlated, processed, or operated on, etc.) upon completion of the contract, including data labeled for training purposes.
d) Model must not access additional services over the internet.

10.2.1.4 Desired Level of Algorithm Rights

a) It is the Government's preference for the selected contractor to provide Government Purpose Rights (the right to use, modify, reproduce, release, perform, display, or disclose technical data within the Government without restriction). This also includes the rights to release or disclose technical data outside of the Government and authorize persons to whom release, or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose technical data for United States government purposes.
b) Respondents may elect to propose alternative options for the Government's consideration.

10.2.2 Integration Compliance Requirements

10.2.2.1 Infrastructure

All systems and services shall meet DHS Enterprise Architecture (EA) policies, standards, and procedures. Specifically, the contractor shall comply with the following Homeland Security (HLS) EA requirements:

a) All developed systems and requirements shall be compliant with the HLS EA principles.
b) All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.

c) All products are subject to DHS EA approval. No products may be utilized in any production environment that are not included in the HLS EA TRM Standards and Products Profile.

d) Description information for all data assets, information exchanges, and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval, and insertion into the DHS Data Reference Model and EA Information Repository.

e) Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.

f) Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications), specific to individual acquisitions, shall be in accordance with the DHS EA (per OMB Memorandum M-05-22, August 2, 2005), regardless of whether the acquisition is for modification, upgrade, or replacement.

g) All EA-related component acquisitions shall be IPv6 compliant, as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

10.2.2.2 Standard Network Compliance Requirements

Proposed solutions must comply with following CBP network engineering requirements:

a) Network traffic from untrusted sources sent into the CBP network shall adhere to the CBP network architecture standards, including but not limited to, firewalls, IDS/IPS, DMZ, etc.

b) No bulk data traffic can be sent to the CBP network without prior knowledge and notification to CBP network personnel.

c) Not initiate network traffic which will oversubscribe CBP network components, violate CBP security policy, or comprise the integrity of the CBP network architecture.

d) Must collaborate with all stakeholders to test all Cloud-related systems and to verify that the systems meet requirements and are able to host applications with no degradation to network performance or security to existing applications in cloud or on Prem.

10.2.2.3 Other Critical Compliance Requirements

The contractor shall comply with the following critical compliance requirements:

a) Accessibility - Section 508 of the Rehabilitation Act requires federal government departments and agencies to ensure all Electronic Information and Technology (EIT) is accessible to people with disabilities. The contractor shall ensure all tasks to design, develop, deploy, operate, and maintain equipment or systems and the systems themselves are in compliance with Section 508 requirements.

b) IT Security Requirements – Ensuring confidentiality, integrity, availability, and authenticity of sensitive data within the DHS IT infrastructure and operations is a foundational element of the CBP mission. The contractor shall ensure that all tasks to design, develop, deploy, operate, and maintain equipment or systems and the systems themselves are in compliance with DHS-4300A. The contractor shall implement multi-factor authentication (Homeland Security Presidential Directive-12, HSPD-12) for network and endpoint device access and ensure that all equipment configurations follow DISA STIGs as required by DHS.

c) Interconnection Security Agreements (ISA) –Interconnection Security Agreements (ISA) are required by DHS policy to establish individual and organizational security responsibilities for the protection and handling of unclassified information. An ISA must be in place to allow connectivity between CBP systems and external participating government agencies and non-government entities via the CBP network. The contractor shall ensure all required ISAs are in compliance with DHS 4300A, and NIST Special Publications SP 800-47 and SP 800-53.

d) Systems Engineering Life Cycle - The DHS SELC is a technical framework that enables consistent management and supports the efficient and effective delivery of capabilities to end-users. The contractor shall ensure that all tasks to design, develop, deploy, operate, and maintain equipment or systems conform to the requirements of DHS Directive 102. The contractor shall adapt all CBP OIT Agile methodologies to comply with DHS SELC requirements, and draft requisite program and technical documentation for all projects per SELC requirements.

e) CBP Enterprise Architecture – The contractor shall ensure that all tasks to design, develop, deploy, operate, and maintain equipment or systems conform to the DHS/CBP Enterprise Architecture (EA), Technical Reference Models (TRM) and other DHS and CBP policies and guidelines including the CBP Information Technology Enterprise Principles and the DHS Service Oriented Architecture - Technical Framework.

f) DHS Geospatial Information Systems – The DHS/CBP Geospatial Vision is to achieve a comprehensive geospatial environment that unifies and supports all mission and business operations with a cohesive approach that includes common operating standards and governance. All geospatial implementations shall comply with the policies and requirements set forth for the DHS Geospatial Information Infrastructure (GII). This includes submission to the Enterprise Architecture Board, or their designee, for review and approval of insertion of hardware, software, services, appliances, and/or structural metadata into the Homeland Security Enterprise Architecture HLS EA.

g) Ensure that all software developed be digitally signed, compiled, and source controlled in CBP's DevOps (DOIT) environment and/or CBP Amazon Web Services Cloud East (CACE) environment for Cloud hosted solutions.

h) CBP business shall be conducted on the CBP network using CBP issued desktop or laptop computers, and CBP email. All data captured and applications developed under the TO shall be stored securely on CBP equipment.

i) Change Management – The contractor shall follow and comply with all CBP OIT and PSPD Change Management processes and procedures to implement software and hardware changes to production systems and applications.

j) The contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

k) The contractor shall provide support for the CBP Information System Security Officer (ISSO) and program stakeholders to comply with CBP procedures, policies and requirements.

10.2.3 DHS-CBP Enterprise Architecture Compliance Requirements

a) The contractor shall ensure that the design conforms to the Department of Homeland Security (DHS) and Customs and Border Protection (CBP) Enterprise Architecture (EA), the DHS and CBP Technical Reference Models (TRM), and all DHS and CBP policies and guidelines (such as the CBP information Technology Enterprise Principles and the DHS Service Oriented Architecture – Technical Framework), as promulgated by the DHS and CBP Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architect (CA).

b) The contractor shall conform to the Federal Enterprise Architecture (FEA) model and the DHS and CBP versions of the FEA model, as described in their respective EAs. All models will be submitted using Business Process Modeling Notation (BPMN 1.1 or BPMN 2.0 when available) and the CBP Architectural Modeling Standards. Universal Modeling Language (UML2) may be used for infrastructure only. Data semantics shall be in conformance with the National Information Exchange Model (NIEM). Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

c) Where possible, the contractor shall use DHS/CBP approved products, standards, services, and profiles, as reflected by the hardware, software, application, and infrastructure components of the DHS/CBP TRM/standards profile. If new hardware, software, or infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal Technology Insertion (TI) process (to include a trade study with no less than four alternatives, one of which reflecting the status quo and another reflecting multi-agency collaboration). The DHS/CBP TRM/standards profile will be updated as TIs are resolved.

d) All developed solutions shall be compliant with the Homeland Security (HLS) EA. All IT hardware and software shall be compliant with the HLS EA.

e) Compliance with the HLS EA shall be derived from an aligned through the CBP EA.

f) Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval, and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

g) Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01. All data-related artifacts will be developed and validated according to DHS Data Management Architectural Guidelines.

h) Applicability of Internet Protocol version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS EA (per OMB Memorandum M-05-22, August 2, 2005) "Selecting Products and Capabilities", regardless of whether the acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant, as defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance, defined in the USGv6 Test Program.

i) In compliance with OMB mandates, all network hardware provided under the scope of this Statement of Work and associated Contracts shall be IPv6 compatible without modification, upgrade, or replacement.

11.0 Access to Unclassified Facilities, Information Technology (IT) Resources, and Sensitive Information

IT resources and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information paragraph 6, describes how contractors must handle sensitive but unclassified information. DHS Sensitive Systems Policy Directive 4300A, and DHS Sensitive Systems Directive, MD 4300A Information Technology Security Program, prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all contracts that require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the contract.

Contractors who require access to the DHS network, such as when conducting remote maintenance, require a background investigation in accordance with DHS Sensitive Systems Directive, MD 4300.A, paragraph 4.1.1.d.

12.0 Personal Identity Verification (PIV) of Contractor Personnel

The contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, paragraph 3, Office of Management and Budget (OMB) guidance M-05-24, Appendix A, chapters 3 and 4, and Federal Information Processing Standards Publication (FIPS PUB) Number 201-2, Personnel Identity Verification of Federal Employees and Contractors, Section 2.

The contractor shall insert this clause in all subcontracts when the subcontractor is required to have routine physical access to a Federally controlled facility or routine access to a Federally - controlled information system.

12.1.1 PIV Credential Compliance

a) Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting Homeland Security Presidential Directorate HSPD-12 PIV credentials as a method of identity verification and authentication.

b) Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and Contractors.

c) PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

d) If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan/or achieving HSPD-12 compliance shall be required/or review, evaluation, and approval by the CISO.

12.1.2 CBP contractor Handling PII Level

When a Contractor, on behalf of CBP, handles, stores, and transmits Sensitive PII data, the contractor shall Accredit (ATO) this information system to the (High-High-Moderate) FIPS level. The contractor shall ensure and certify that they will not retain any PII on non CBP systems.

Contractor employees shall satisfy the Privacy Training requirement by completing the training at **http://www.dhs.gov/dhs-security-and-training-requirements-contractors.** Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter, not later than October 31st of each year.

13.0 Accessibility Requirements (Section 508 Compliance)

Section 508 of the Rehabilitation Act (classified to 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Appendixes A, C & D, and available at https://www.ecfr.gov/cgi-bin/text-idx?SID=e1c6735e25593339a9db63534259d8ec&mc=true&node=pt36.3.1194&rgn=div5. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards. ICT includes IT and other equipment.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018, or any successor publication.

13.1 Section 508 applicability to Information and Communications Technology (ICT): Anomaly Detection Algorithm

a) Applicable Exception: Fundamental Alteration Authorization #**:** CBP-20140703-001
   Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018, or any successor document.

14.0 DHS Information Technology Portfolio Alignment

The system shall align with the DHS IT Portfolio below:

a) **Screening/Watchlist/Credentialing** includes all activities that support the tracking and monitoring of travelers, conveyances and cargo crossing U.S. borders, and traffic pattern analysis, database (Federal, State, and Local) linking and querying, and managing status verification and tracking systems. Different investments and systems may support distinct screening and watchlist activities for people, cargo, and tangible goods. Credentialing encompasses all activities that determine a person's eligibility for a particular license, privilege, or status, from application for the credential through issuance, use, and potential revocation of the issued credential.

15.0 Supply Chain Risk Management Terms and Conditions

a) The Contractors supplying the Government hardware and software shall provide the manufacturer’s name, address, state or domain of registration, and the Data Universal Numbering System (DUNS) number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state or domain of registration and DUNs number of those suppliers must also be provided.

b) Subcontractors are subject to the same general requirements and standards as prime Contractors. Contractors employing subcontractors shall perform due diligence to ensure that these standards are met.

c) The Government shall be notified when a new Contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.

d) Contractors shall provide, implement, and maintain a Supply Chain Risk Management Plan in the Contractor’s format that addresses internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, components, and software. The Supply Chain Risk Management Plan shall include a list of custom or non-standard parts used by the Contractor.

e) The Plan shall describe the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this contract.

f) The Supply Chain Risk Management Plan shall address the following elements:
   1. How risks from the supply chain will be identified,
   2. What processes and security measures will be adopted to manage these risks to the system or system components, and
   3. How the risks and associated security measures will be updated and monitored.

g) The Supply Chain Risk Management Plan shall remain current through the life of the contract or period of performance. The Supply Chain Risk Management Plan shall be provided to the Contracting Officer Representative (COR) 30 days post award.

h) The contractor acknowledges the Government’s requirement to assess the Contractors Supply Chain Risk posture. The contractor understands and agrees that the Government retains the right to cancel or terminate the contract, if the Government determines that continuing the contract presents an unacceptable risk to national security.

i) The contractor shall disclose, and the Government will consider, relevant industry standards certifications, recognitions and awards, and acknowledgments.

j) The contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the Contracting Officer (CO). Contractors shall only provide Original Equipment Manufacturers (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.

k) The contractor shall be excused from using new OEM (i.e., "grey market," previously used) components only with formal Government approval. Such components shall be procured from their original genuine source and have the components shipped only from manufacturers authorized shipment points.

l) For software products, the contractor shall provide all OEM software updates to correct defects for the life of the product (i.e., until the "end of life"). Software updates and patches must be made available to the government for all products procured under this contract.

m) Contractors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill contract obligations with the Government.

n) All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lesser of the term of the contract, the period of performance, or one calendar year from the date the activity occurred.

o) These records must be readily available for inspection by any agent designated by the

p) U.S. Government as having the authority to examine them.

q) This transit process shall minimize the number of times in route components undergo a change of custody and make use of tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

r) The contractor is fully liable for all damage, deterioration, or losses incurred during shipment and handling, unless the damage, deterioration, or loss is due to the Government. The contractor shall provide a packing slip which shall accompany each container or package with the information identifying the contract number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact. The contractor shall send a shipping notification to the intended government recipient or contracting officer.

s) This shipping notification shall be sent electronically to nii.cor@cbp.dhs.gov and will state the contract number, the order number, a description of the hardware/software being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number