Work Statement Attachment - Information Technology Security Requirements Summary

NOTE: Provide the appropriate information for the below items. Leave "Not applicable" entry in items that do not pertain to this purchase.

1. Background Investigation

Contractor employees who will have access to Federal information technology (IT) systems are subject to background investigations by the Federal Office of Personnel Management. Procedures for investigations and obtaining identity credentials are described in clause GS 1414 (or GS 1419 if working on the Denver Federal Center). The level of investigation required will be the same as would be required for Federal employees holding positions involving similar duties.

Based on the risk and sensitivity of duties performed and system access authorities to be granted, the following type of background investigations will be required, as described in DOI Departmental Manual Part 441, Chapter 3, Attachment 5 (available at: http://elips.doi.gov/app_dm/act_getfiles.cfm?relnum=3631).

Duties – develop automated training and inference pipeline for the USGS Flow Photos Explorer.

Investigation Level – *1*

2. Non-disclosure Agreement

Prior to receiving access to USGS computers, contractor employees shall be required to sign non-disclosure or other system security agreements, depending on the systems to be used and level of access granted. The required non-disclosure agreement will be similar to the attached but may be customized, as needed, to reflect the data involved. Restrictions on use, duplication, and disclosure of sensitive and proprietary data are covered in clause GS 1406.

3. Training

Contractor employees shall complete USGS-defined Federal Information Systems Security Awareness computer security training before being granted system access and must renew the training annually. Failure to complete training within the required timeframe may result in loss of system access for that user. Contractor employees with significant IT security responsibilities shall also complete specialized role-based training.

4. Personnel Changes

Before starting work, the contractor will provide a listing to the COR/technical liaison identifying contractor and subcontractor employees requiring access to USGS systems for performance of work hereunder and will assign each person a unique user ID. The contractor shall immediately advise the USGS Project Officer when any of their personnel no longer require USGS computer access so that those ID's and access privileges can be cancelled. The COR must be notified in advance of any potentially unfriendly termination of an employee or subcontractor.

5. Contractor Location

No portion of the services to be performed hereunder may be performed outside the United States without the express written permission of the Contracting Officer. If a contractor proposes to perform services outside the United States, the contractor must submit a Security Plan to address mitigation of security issues due specifically to location. The Security Plan Template is available upon request from the Contracting Officer. Such proposals will not be accepted unless the contractor can demonstrate that the Government systems or data would be no more vulnerable than if work were performed domestically.

6. Applicable Standards

7. Asset Valuation

Not applicable

8. Property Rights

Not applicable

9. Independent Verification and Validation (IV & V)

Not applicable

10. Certification & Accreditation

Not applicable

11. Internet Logon Banner

Not applicable

12. Incident Reporting

Contractor employees must report any computer security incidents (viruses, intrusion attempts, system compromises, offensive e-mail, etc.) which may affect Government data or systems in accordance with the *DOI Computer Incident Response Guide*. Report computer security incidents to USGS help desk or Security Point Of Contact (SPOC). In many cases, your local system administrator is your Security Point Of Contact. The help desk or SPOC will investigate and coordinate with the *Computer Security Incident Response Team (CSIRT)*.

13. Quality Control (Malicious Code)

All software and hardware shall be free of malicious code.

14. Self Assessment

Self-assessment on USGS systems to which the Contractor may have access under this contract will be conducted by the Government or another of its contractors.

15. Vulnerability Analysis

Vulnerability Analysis on USGS systems to which the Contractor may have access under this contract will be conducted by the Government or another of its contractors.

16. Logon Banner

Not applicable

17. Security Controls

Not applicable

18. Contingency Plan

Not applicable