NGA BIG-R BAA HM047620BAA001

TOPIC 6: Detecting Known Trajectory Manipulations (DKTM)

1. Publication and Changes History:

Date	Description
03/29/2022	Topic Posting – BIG-R BAA Topic 6 Version 1

2. Available Funding:

2.1. Phase I:

- Up to $1.7M
- It is the Government's intent to make up to three (3) Phase I awards within the 1.7M budget

2.2. Phase II:

- Up to $1M
- It is the Government's intent to down-select and make one (1) Phase II award within the $1M budget

3. Due Dates & Posting Locations

	Date	Time	Posting Location
Questions Submission	04/05/2022	5:00pm ET	Classified ARC
Q&A Posting	04/14/2022		Classified ARC
Abstract Submission	04/25/2022	5:00pm ET	Classified ARC
Abstract Feedback	05/10/2022		Classified Email
Proposal Submission	06/01/2022	5:00pm ET	1. **Full Proposal**: Classified ARC **AND** 2. **Unclassified Volumes**: BigRBAA@nga.mil (Email Subject: 'TOPIC 6 – DKTM Unclassified Proposal Volumes')

4. Point of Contact (POC)

For questions please contact the Contracting Officer (CO): Daniela Garavito

Email Address:

- **Unclassified**: **BigRBAA@nga.mil**
- **Classified**: **NGABigRBAA@coe.ic.gov**
  - (→ Shall send unclassified email to inform CO of classified messages.)

➔ Use the following email subject for all email correspondence: **'TOPIC 6 – DKTM'**

5. Classified ARC Access Required

In order to view **Attachment 1** on the classified ARC website, you must have a TS/SCI clearance.

Access to this effort will require a classified ARC account. To create a classified ARC account, you must first create an unclassified ARC account by visiting https://acq.westfields.net and clicking on the "Register" link at the top right of the page. Be sure to include your classified email address as you will not be able to access your classified account without it. Once you have finished the registration process on the unclassified systems and validated your account by clicking the link you were sent via email, you will need to wait 2 business days for your classified ARC account to be automatically created.

Once you have waited 2 business days, you will be able to log into your classified account using the same email and password you used on the unclassified system. This will bring you to a page where you can click a button to send yourself a verification email to the classified email account you listed when creating your unclassified account. To log into the classified ARC, visit https://acq.nro.ic.gov from a TS network such as NMIS, NSAnet, CWE, AWAN, CWAN, JWICS, etc. If you do not have access to a TS network but possess a TS/SCI clearance, you can arrange a visit to our reading room by calling (703) 230-6100.

6. Background & Purpose

Over twenty years ago in a report published by the National Transportation Safety Council it was theorized that it would be possible to intentionally misdirect a Global Positioning System (GPS) receiver using only a few synthesized Radio Frequency (RF) signals created to mimic actual Global Navigation Satellite System (GNSS) GPS signals [1]. It was suggested the purpose of the hypothetical mimic would be to corrupt the capacity of any targeted GPS receiver to produce accurate geo-coordinate information. In 2008, in the United States, one American academic researcher demonstrated that a digital signal processing device connected to a suitable RF transmitter could indeed force a standard GPS receiver to produce false (or spoofed) geo-coordinate output [2].

➔ **See Attachment 1 on Classified ARC for further details on Background & Purpose**

Attachment 1 shall be reviewed before submitting any questions, abstracts, or proposals.

7. Scope & Mission

The National Geospatial-Intelligence Agency (NGA) Office of Research is looking for a capability that can recognize suspected GPS-derived geo-coordinate manipulations in large sets of spatio-temporal trajectory data.

The mission of DKTM is to bring to NGA technology capable of:

- processing large, geo-coordinate data sets having time and identifier metadata
- inferring spatial trajectories from the geo-coordinate data sets aggregated by identifier
- automating the process of finding trajectory manipulations
- reporting to a user the discovery of the manipulations found in the data

➔ **See Attachment 1 on Classified ARC for further details on Scope & Mission**

Attachment 1 shall be reviewed before submitting any questions, abstracts, or proposals.

8. Metrics & Milestones

➔ **See Attachment 1 on Classified ARC for further details on Metrics & Milestones**

Attachment 1 shall be reviewed before submitting any questions, abstracts, or proposals.

9. Deliverable Items

9.1. Phase I – Deliverables

For both Phase I and Phase II the performer shall participate in a project kick-off briefing, a mid-point briefing, and a close out briefing, in each Phase respectively. The purpose of these briefings is a bilateral (NGA – performer) sharing of NGA requirements and information, performer results, and to update all associable metrics and scheduling information.

Phase I Deliverables

ITEM	DESCRIPTION	DUE DATE
Kick-off Briefing	• A performer hosted, potentially virtual, NGA briefing to the performer wherein the NGA communicates to the performer final details of schedule and performance expectations, and NGA internal points of contact for obtaining relevant GPS-based trajectory data.	7-Days after contract award
Monthly Status Reports	• A performer hosted, potentially virtual, performer briefing to the NGA wherein the NGA will give guidance to the performer in order to ensure that the performer is on the right track. This briefing will be accompanied by a written report.	First of each month begins month 2
	• Each report will provide NGA a summary of the work accomplished during the previous month, any challenges or issues that could impact the next month, plus a brief summary of intended actions for the following reporting period. Not to exceed 5 – 10 pages.	
Mid-point Review	• A performer hosted, potentially virtual meeting that informs NGA of performer project progress, operating prototype software, and communicates the quantitative status of Phase I work. • The performer will deliver correctly operating detection algorithms addressing data corruptions in Set 1 listed within Attachment 1 of this document. This will include all source code, all libraries, dependencies, prototype software documentation, user manuals, and compiler recommendations. The algorithm(s) delivered will be capable of detecting each of the Set 1 trajectory manipulations of interest to DKTM. • The performer will demonstrate their original prototype software's capability of detecting each of the Set 1 trajectory manipulations of interest to DKTM.	Contract award + 6 months

ITEM	DESCRIPTION	DUE DATE
	• NGA will test the performer's correctly operating detection algorithm(s) in-house using NGA GPS-based trajectory data sets.	
Algorithm(s)	• The performer will deliver to the NGA correctly operating detection algorithms capable of detecting *all* trajectory manipulations of interest (see Attachment 1) to DKTM and a trajectory 'shape detection' utility that can be parameterized to find previously unknown, i.e., new, geometric shapes. • Algorithms will be delivered to NGA as source code with a complete specification of algorithm(s) operation, all necessary libraries, dependencies, and compiler recommendations. • The performer will verify that all delivered source code, libraries, and dependencies will be cleared to operate on a classified computer network • NGA will test the performer's correctly operating detection algorithm(s) in-house using NGA GPS-based trajectory data sets. • The performer will provide NGA with a standard IEEE 1016 Software Description Document (SDD) written from the viewpoint of DKTM use-cases and known algorithm weakness where each manipulation detection algorithm will be addressed. Those sections in the SDD devoted to describing each manipulation detection algorithm will be two to five pages in length.	45-days before end of phase
Validation and Verification (V&V) Plan	• Describe a methodology, preferably an automated method or theoretic (deterministic equation) that can be used to evaluate the performance of the correctly operating detection algorithm(s).	
Final report	• Final technical report summarizing the work performed and the final results of the effort. Not to exceed 10 – 15 pages.	(U) 7-days before end of phase
Close-out briefing	• Final briefing to the Government on project results.	

9.2. Phase II - Deliverables

Phase II Deliverables

ITEM	DESCRIPTION	DUE DATE
Kick-off Briefing	• A performer hosted, potentially virtual, NGA briefing to the performer wherein NGA communicates to the performer final details of schedule and performance expectations, and NGA internal points of contact for obtaining relevant GPS-based trajectory data. • A service-oriented architecture (SOA) application program interface (API) descriptive contract will be supplied to the performer in PDF format.	7-Days after contract award
Review	• Periodic and unscheduled reviews will take place throughout the period of performance in order to ensure that the development of the desired interface and an environment that is suitable for analysts.	Monthly and unscheduled
Algorithms	• All DKTM correctly operating detection algorithms operating as one or more back-end server processes interfaced through a RESTful SOA API to an NGA client user interface.	(U) 60-days before end of phase (month 10)
Training Video	• A web-based training video demonstrating the theory and use of the DKTM prototype software on NGA data.	(U) 30-days before end of phase (month 11)
Source Code, Libraries Manuals, & Compiler Recommendations	• All DKTM source code with a complete specification of all necessary libraries, dependencies, user manuals, and compiler recommendations. • The performer will provide NGA with a standard IEEE 1016 SDD written from the viewpoint of DKTM use-cases and known algorithm weakness where each manipulation detection algorithm will be addressed. Those sections in the SDD devoted to describing each manipulation detection algorithm will be two to five pages in length.	
Final report	• Final technical report summarizing the work performed and the final results of the effort. Not to exceed 10 – 15 pages.	(U) 7-days before end of phase
Close-out briefing	• Final briefing to the government on project results.	

10. Operating Constraints

Successful proposals offered to Topic 6 will include a description and schedule of work planned in both Phase I and Phase II as well a discussion of the algorithm(s) intended to identify the trajectory manipulations of interest to DKTM. The goal of Topic 6 is to identify and place under contract performers from the several fields of mathematics, engineering, computer science, social science, and or 'other' associable communities of interest capable of helping NGA automate the discovery and recognition of anomalous trajectory manipulations.

Performers are highly encouraged to create code that is extensible and capable of identifying additional manipulations not listed in Attachment 1. The successful performer will explicitly describe an algorithmic method to create a trajectory manipulation 'shape detection' utility that is parameterizable.

NGA is aware that in many cases the detection and identification of a trajectory manipulation will require spatial, temporal, and or possibly social context. Thus, proposers are encouraged to be creative in their approach to solving the DKTM problem. This might include but would not be limited to integrating the proposer's original prototype software with mapping engines and or information service engines that are approved for use on a classified computer network.

11. Government Furnished Information (GFI)

NGA has access to large data sets of GPS-based trajectory data. Successful performers will be put in contact with NGA staff specially trained to assist in facilitating large data set access and transfer.

These data sets are typically ASCII text based, comma separated value files. A single file containing these data may be a few thousand bytes or several million bytes long. The proposer will be the best judge on how large a data set they will need from NGA to complete their deliverable(s).

12. Security Considerations

It is anticipated that performers working on the DKTM project and their computing hardware/ software tools and resources will need to support work up to TS/SCI.
GPS-based trajectory data supplied to the performer by the NGA may be classified up to TOP SECRET//SI//TK//NOFORN.

12.1. Classified Work Performance Security Requirements

12.1.1. Contractor personnel performing Top Secret/Sensitive Compartmented Information (TS/SCI) work on the contract are required to have active TS/SCI clearances for access to NGA facilities, when performing duties within TS/SCI environments, and for access to TS/SCI NGA computer systems. Contractors are subject to a Counterintelligence Scope Polygraph, as requested by the Government. All Contractor personnel shall possess a current Top-Secret Personnel Security Clearance and be eligible for favorable NGA adjudication for SCI access. The government will be responsible for verifying security clearances/SCI eligibility of the Contractor personnel IAW Security Executive Agent Directive (SEAD) 7: "Reciprocity of Background Investigations and National Security Adjudications". NGA will sponsor SCI accesses, NGA Badges, Common Access Cards (CAC) and other items (e.g. parking hangtags) when applicable, for required contract personnel.

12.1.2. Contractors must abide by the DD Form 254 - Contract Security Classification Specification and applicable security policies and regulations.

12.1.3. Contractor personnel shall follow all applicable NGA, IC, and DoD information security and operational security policies and guidance during performance of contract requirements.

12.1.4. The Contractor shall inform the Government when its employees no longer support the contract (see DD254). The Government desires notification prior to the day the individual no longer supports the contract, but requires notification no later than the day support ends. If Contractor personnel will no longer be supporting NGA via an NGA contract, any debriefing paperwork, notifications, and/or requests for further direction from the COR or Industrial Security shall be turned into the NGA Workforce Support Center, NGA Site Security Office, or the COR. If Contractor personnel are unable to turn these items into the NGA Workforce Support Center, NGA Site Security Office, or COR then it is the Contractor's security office's responsibility to collect the items from the individual. If the Contractor debriefs the employee, the Contractor shall send a copy of the debriefing statement, plus any Government items (e.g. NGA Badge, CAC, Courier Card, parking hangtags, etc.) within four (4) business days (timeline may be extended with authorized documented exceptions by NGA Security) to an NGA Site Security Office or the NGA Workforce Support Center.

12.1.5. All classified work performed at a non-NGA facility must be approved by the COR. Any classified work performed at collaborator sites must be performed in either an NGA

accredited SCIF or an Other Government Agency (OGA) SCIF that has either a Memorandum of Agreement (MOA), Memorandum of Understanding (MOU), Joint Use Agreement or Co-Use Agreement with NGA for this contract.

12.1.6. Cleared Contractor personnel may hand-carry contract-related classified information as authorized by the COR. Contractor personnel will obtain NGA courier authorization prior to hand-carrying of contract-related classified information. Contractor personnel will be limited to hand-carrying classified information between the Contractor facilities and NGA facilities only.

12.1.7. Cleared Contractor personnel will be enrolled into Director of National Intelligence (DNI) Continuous Evaluation System (CES) throughout the lifecycle of the contract while at NGA IAW SEAD 6: "Continuous Evaluation". Cleared Contractor personnel must self-report security issues, foreign contacts, and other reporting requirements in accordance with SEAD 3: "Reporting Requirements for Personnel With Access to Classified Information or Who Hold a Sensitive Position" and NGA Instruction 5205.3, "Security Reporting Requirements". In addition, cleared Contractors will be required to submit electronic fingerprints and will be enrolled into NGA's Report of Arrest and Prosecution Background (RAPBack) program, which supports CES.

12.1.8. Cleared Contractor personnel, who are designated as Tier 3 Privileged Users or holding enhanced access through a Special/Controlled Access Program (SAP/CAP), will be required to participate in NGA's annual Security Financial Disclosure Program (SFDP) as directed by D/NGA in the 20 November 2020 memorandum titled "Designation of NGA Personnel Required to Participate in the Security Financial Disclosure Program.

12.2. Unclassified Work Performance Security Requirements

12.2.1. Uncleared Contractor personnel are authorized to work on this contract up to the Unclassified level, with access to DoD Controlled Unclassified Information (CUI) at the Contractor site without the requirement of a security clearance.

12.2.2. Any Contractor personnel working with CUI information must receive a favorable HSPD-12 and/or HSPD-12 Tier 1 adjudication prior to accessing CUI information. Contractor personnel who require access to CUI for 60 days or less must receive a favorable HSPD-12 adjudication. Contractor personnel who require CUI access for greater than 60 days must receive a favorable HSPD-12 Tier 1 adjudication.

12.2.3. NGA will sponsor the HSPD-12 and HSPD-12 Tier 1 background investigation for required program personnel. NOTE: Contractor personnel submitted for SCI access cannot be submitted for a HSPD-12 or HSPD-12 Tier 1 adjudication while waiting for their SCI approval.

12.2.4. Foreign nationals *are not* permitted to perform unclassified work under the terms of this contract.

12.2.5. Contractor personnel shall not release any unclassified information, regardless of medium (e.g. film, tape, document), pertaining to any part of this contract or any program related to this contract, unless the COR has given prior written approval or in performance of a project that has been scoped and negotiated by NGA.

12.2.6. Contractor personnel visiting NGA facilities and/or sites will receive the appropriate visitor badge and be escorted, as appropriate. The visitor badge will be returned at the end of each visit day. NOTE: NGA reserves the right to refuse access to any personnel.

12.2.7. Contractor personnel are forbidden from bringing in prohibited, unauthorized, and/or Portable Electronic Devices (PEDs) items into any NGA installation or any secure office/working location covered under this agreement. A list of PEDs includes but is not limited to cell phones, cameras, two-way pagers, laptops, recorders (e.g. digital, tape, etc.), flash drives, or any other kind of removable media, without prior approval and approval paperwork from NGA. See NGA instructions/regulations/policy for a full list of prohibited and unauthorized items. Security violation repercussions will be determined on the severity of the violation.

12.3. Information Handling

12.3.1. Contractor personnel will comply with the NGA, DoD, and IC policies and regulations (to include, but not limited to, the Consolidated NGA (CoNGA) Security Classification Guide) to properly mark (to include portion marking) classified and unclassified documentation, media, etc.

12.3.2. Document markings will be in accordance with the lowest security classification possible to ensure the confidentiality and integrity for the greatest release to partners in accordance with NGA and mission partner marking guides for classified information.

12.3.3. All Government-furnished information released to the Contractor or created in the performance of this contract will be destroyed or returned by the Contractor to NGA upon contract termination or when no longer required for contract performance. The determination to destroy or return will be at the direction of the NGA CO or COR.

13. Proposal Volume 4 - Security Requirements (Topic 6)

The following paragraphs list additional requirements to

BIG-R BAA General Solicitation, Part IV "Abstract and Proposal Submission Information", Section 6.3.4 Volume 4 "Administrative and National Policy requirements", Part iv. "Security Requirements":

The security volume must demonstrate the Proposer's ability to meet the security requirements of the solicitation in accordance with the DD Form 254 (Attachment 2) and this topic call, which will enable minimal contract transition at the time of award to full performance of the effort. The security volume will not include proposed subcontractor(s) information, as the Proposers will be responsible for ensuring that its subcontractor(s) meet(s) security requirements in accordance with the DD Form 254 and applicable security policies and regulations. The security volume must provide sufficient information for the Government to evaluate the Security Sub-Factors set forth in Section 14 of this document at the time of proposal submission.

The Security volume must specifically contain the below information:

1. Facility Clearance (FCL) and Foreign Ownership, Control, or Influence (FOCI)
2. Personnel Security Clearance Level (PCL)/ Sensitive Compartmented Information (SCI) access
3. Sensitive Compartmented Information Facility (SCIF)
4. Security Plan
5. Supply Chain Risk

13.1. Facility Clearance (FCL) and Foreign Ownership, Control, or Influence (FOCI)

The security volume must provide the following information on the Proposer's FCL using the Facility Clearance Level template at Attachment 3:

- Company Name
- Address and Zip Code
- Commercial and Government Entity (CAGE) Code
- Facility Clearance Level

If the Proposer is a small business joint venture and if 13 Code of Federal Regulations (C.F.R.) 121.103(h)(4) applies, "Proposer" includes the "joint venture itself or the individual partner(s) to the joint venture that will perform the necessary security work."

The security volume must provide a copy of the most recently adjudicated signed, dated, witnessed or notarized Certificate Pertaining to Foreign Interest (SF 328) for the FOCI evaluation. If any of the responses on the SF 328 are "yes", the Offer must submit official communications documentation from Defense Counterintelligence and Security Agency (DCSA)

that corresponds with the CAGE code(s) and most recently adjudicated SF 328 form submitted that authorizes the company's FCL with FOCI. Official communications documentation can be in the form of a letter on DCSA letterhead, a memorandum from DCSA with DCSA logo or letterhead, or an email communication from DCSA showing date/time stamp and official DCSA email address. In lieu of documentation from DCSA, the Proposer must submit a screen capture of their current FCL status as reflected in the National Industrial Security System (NISS) that corresponds to the CAGE code(s) submitted. The screen capture must display a date that is no more than thirty (30) days before the date of the proposal submission.

Per C.F.R. 32 Part 117.11, National Industrial Security Program Operating Manual (NISPOM), the Cognizant Security Authority (CSA) will consider a U.S. entity to be under FOCI when a foreign interest has the power to direct or decide issues affecting the entity's management or operations in a manner that could either result in unauthorized access to classified information; or adversely affect performance of a classified contract or agreement. The U.S. entity may also be considered to be under FOCI when a foreign interest or government is currently exercising, or could exercise, that power, whether directly or indirectly, such as through ownership of the U.S. entity's securities, by contractual arrangements, or other means. When a CSA has determined that an entity is under FOCI, the primary consideration will be the protection of classified information. The CSA will take whatever action is necessary to protect classified information, in coordination with other affected agencies as appropriate.

NOTE: Proposers (prime contractor, sub-contractor, or small business joint venture member, if applicable) that have an FCL arrangement under a Special Security Agreement (SSA) and require a National Interest Determination (NID) for access to proscribed information shall not gain access to such information until the NID is properly executed by the Government. Proscribed information is identified in 32 C.F.R. §2004.22 and includes Top Secret, COMSEC, SCI, Special Access Programs and Restricted Data. This applies to pre and post award access.

13.2. Personnel Security Clearance (PCL)/Sensitive Compartmented Information (SCI) access

The security volume shall contain a listing of the proposed key personnel, i.e., Principle Investigator(s) (PIs), required by the solicitation with the information indicated below using the Personnel Security Clearance template as Attachment 4:

- Full Name (Last, First, Middle)
- Name of current employer
- Date of Birth
- Place of Birth
- Social Security Number (SSN) *
- Current Investigation (Type and Date)
- SCI Adjudication (Eligibility) Date
- Government Sponsor

***NOTE:** Directive-Type Memorandum (DTM) 2007-015-USD (P&P) – DoD Social Security Number (SSN) Reduction Plan (and references) - Security Clearance Investigation or Verification and NGA NI 5401.1: Privacy and Civil Liberties Program - The initiation, conduct, or verification of security clearances requires the use of SSN. The SSN is the single identifier that links all of the aspects of these investigations together.*

Personnel Security Clearance information shall be provided as a separate attachment, encrypted/password protected, and properly marked with the following verbiage; "*The document contains Personally Identifiable Information (PII) and is For Official Use Only. Unauthorized dissemination or use of PII is a violation of Federal Law. Individuals in violation may be subject to fines, disciplinary actions, or both (P.L. 93-579).*"

13.3. Sensitive Compartmented Information Facility (SCIF)

The security volume shall contain a copy of the most recently issued SCIF accreditation letter for each SCIF location where the Proposer proposes to perform SCI work under this Contract and specifically identify the Cognizant Security Authority of the sponsoring agency. If the Prime Proposer proposes to use a SCIF under the control of another private party, the security volume must describe in detail the arrangements that have been made to do so.

13.4. Security Plan

The security volume shall include a security plan that demonstrates how the Proposer will protect classified (Collateral and SCI) material in accordance with Department of Defense (DoD), and Director of National Intelligence (DNI), security policies and regulations for this effort. At a minimum, the security plan must demonstrate an understanding of the Government's requirement by addressing: (1) the pre-screening of individuals for clearances/accesses; (2) security training requirements; (3) a comprehensive approach to the protection and safeguarding of classified/sensitive information; (4) a plan to manage threats to the supply chain from foreign interference; and (5) procedures for handling security incidents and/or violations.

13.5. Supply Chain Risk

NGA will assess a Proposer's Supply Chain Risk, under the authority of Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 239.73 and in accordance with guidance provided by Intelligence Community Directive (ICD) 731, Supply Chain Risk Management, Intelligence Community Standard (ICS) 731-02, Supply Chain Threat Assessments, National Institute of Standards and Technology (NIST) Special Publication 800- 161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, and all other instructions or directives applicable to NGA and its contractors, including but not limited to: DoD Instruction (DoDI) 5200.44 "Protection of Mission Critical Functions to Achieve Trusted

Systems and Networks (TSN)," DoDI 5000.83 "Technology and Program Protection to Maintain Technological Advantage," and NGA Instruction (NGAI) 5050.1, "Supply Chain Risk Management."

Supply Chain Risk will be assessed using the entire submitted proposal and requires no additional submission related to Prime and Subcontractor information beyond what is requested above. Information that may be reviewed by the Government in this assessment includes, but is not limited to, submitted CAGE codes, DUNS number, SF-328 and attachment(s), proposed key personnel, identified subcontracts, and the security plan. Additionally, the Government may use the authorities provided by section 10 U.S.C. 2339a to consider information, public and non-public, including all-source intelligence, relating to an Proposer and its supply chain.

14. Evaluation – Volume 4 - Security (Topic 6)

The following paragraphs list additional requirements to

BIG-R BAA General Solicitation, Part V: "Abstract and Proposal Review Information", Section 3.2.4 "Step 4: Security Evaluation":

Security Factor – (Pass/Fail)

The Government will evaluate information provided in the Proposer's proposal on a Pass/Fail basis at the time of proposal submission to determine security eligibility and the ability to satisfy the requirements set forth in the DD Form 254, and an assessment of the Proposer's security plan submitted in its proposal explaining how the Proposer will comply with security policies and regulations. The Proposer must provide information that can be verified via NGA, DoD, and/or IC databases and/or through coordination with other DoD and IC agencies, as applicable.

There are five (5) security Sub-Factors which will be used to evaluate the Security Factor:

- **Security Sub-Factor 1:** Facility Clearance (FCL) and Foreign Ownership, Control, or Influence (FOCI)
- **Security Sub-Factor 2:** Personnel Security Clearance Level (PCL)/ Sensitive Compartmented Information (SCI) access
- **Security Sub-Factor 3:** Sensitive Compartmented Information Facility (SCIF)
- **Security Sub-Factor 4:** Security Plan
- **Security Sub-Factor 5:** Supply Chain Risk

14.1. Security Sub-Factor 1: Facility Clearance (FCL) and Foreign Ownership, Control, or Influence (FOCI)

The Proposer's proposal will be evaluated, via a database query, to determine whether the Proposer, at the time of the security volume submission, possesses an active Top Secret FCL (Facility Clearance shown on DD Form 254).
The Proposer must:

(1) demonstrate that there are no unmitigated FOCI issues or concerns (all "no" answers to SF 328); or, when there are "yes" answers,
(2) include official communications from DCSA authorizing their FCL with FOCI; or
(3) provide a screen capture of their NISS Facility Profiles tab displaying their current status as having no unmitigated FOCI issues in conjunction with their SF 328 (that displays "yes" answers).

13 C.F.R. 121.103(h)(4) will be applied when the Government evaluates the proposal under this Sub-Factor if the Proposer is a small business joint venture. Thus, if applicable, "Proposer" includes the "joint venture itself or the individual partner(s) to the joint venture that will perform the necessary security work."

The below Pass/Fail ratings will be applied to determine if the Security volume passes or fails Sub-Factor 1: Facility Clearance (FCL) and Foreign Ownership, Control, or Influence (FOCI)

Table M.1 Rating for FCL / FOCI

FCL/FOCI Rating	Description
Pass	This Sub-Factor is met when: (1) NGA Acquisition Security verifies, via a database query, that the Proposer possesses, at time the security volume is submitted, an active Top Secret FCL and (2) all identified FOCI issues and concerns have been properly mitigated in accordance with the NISPOM (with official DCSA documentation or NISS screenshot submitted).
Fail	This Sub-Factor is not met if: (1) NGA Acquisition Security is unable to verify, via a database query, that the Proposer possesses, at time the security volume is submitted, an active Top Secret FCL and/or (2) all FOCI issues and/or concerns have not been properly mitigated in accordance with the NISPOM (or the Proposal fails to provide the appropriate documentation).

14.2. Security Sub-Factor 2: Personnel Security Clearance Level (PCL)/ Sensitive Compartmented Information (SCI) access

The Security Volume will be evaluated, via a database query, to determine that each key personnel, i.e., Principle Investigator(s), (as required by the RFP) proposed by the Proposer, demonstrates a favorably adjudicated Top Secret/SCI Access Eligibility that:

1) is not more than seven years old; or has been entered into the Continuous Evaluation program with a deferred investigation requirement, and
2) meets the reciprocity requirements of Security Executive Agent Directive 7 (SEAD 7).

The below Pass/Fail ratings will be applied to determine if the Security volume passes or fails Sub-Factor 2: Personnel Security Clearance (PCL)/ Sensitive Compartmented Information (SCI) access.

Table M.2 Rating for PCL

PCL Rating	Description
Pass	This Sub-Factor is met when: NGA Acquisition Security verifies, via a database query, that the Proposer's proposed key personnel meet the requirement as stated in Sub-Factor 2. [NOTE: Proposed personnel with waivers, conditions, or deviations assigned to access eligibility will be accepted for consideration during source selection; however, after award, NGA Personnel Security may determine the waiver, condition, or deviation poses an unacceptable National Security risk for NGA and not accept the waiver, condition or deviation.]
Fail	This Sub-Factor is not met if: NGA Acquisition Security is unable to verify, via a database query, if one or more of the Proposer's proposed key personnel meet the requirement as stated in Sub-Factor 2.

14.3. Security Sub-Factor 3: Sensitive Compartmented Information Facility (SCIF)

The Security volume will be evaluated to determine the Proposer's ability, by 07/01/2022, to utilize an accredited SCIF (or SCIFs) that can be properly covered by a Government approved Co-Utilization agreement and/or otherwise meets DoD or ODNI SCIF security requirements to accomplish SCI work that must be performed (or is otherwise proposed to be performed) under this Contract.

The below Pass/Fail ratings will be applied to determine if the Security volume passes or fails Sub-Factor 3: Sensitive Compartmented Information Facility (SCIF)

Table M.3 Rating for SCIF

SCIF Rating	Description
Pass	This Sub-Factor is met when: NGA Acquisition Security verifies, through database queries and/or coordination with other DoD and IC agencies, as applicable, that the Prime Proposer's proposed SCIF (or SCIFs) meets all accreditation requirements as stated in Sub-Factor 3.
Fail	This Sub-Factor is not met if: NGA Acquisition Security is unable to verify, through database queries and/or coordination with other DoD and IC agencies, as applicable, that the Prime Proposer's proposed SCIF (or SCIFs) meets all accreditation requirements as stated in Sub-Factor 3.

14.4. Security Sub-Factor 4: Security Plan

The Security volume will be evaluated for the Proposer's approach to protect classified (collateral and SCI) information in accordance with DoD, and DNI, security policies and regulations for this effort. At a minimum the security plan must demonstrate an understanding of the Government's requirement by addressing:

(1) the pre-screening of individuals for security clearances/accesses;
(2) security training requirements;
(3) a comprehensive approach to the protection and safeguarding of classified/sensitive information;
(4) a plan to manage threats to the supply chain from foreign interference; and
(5) procedures for handling security incidents and/or violations.

The below Pass/Fail ratings will be applied to determine if the Security volume passes or fails Sub-Factor 4: Security Plan

Table M.4 Rating for Security Plan

Security Plan Rating	Description
Pass	This Sub-Factor is met when: The Proposer's security plan addresses all required topics and demonstrates an understanding of the Government's requirements as stated in Sub-Factor 4.
Fail	This Sub-Factor is not met if: The Proposer's security plan does not address all required topics and/or does not demonstrate an understanding of the Government's requirements as stated in Sub-Factor 4.

14.5. Security Sub-Factor 5: Supply Chain Risk

The Government will assess a Proposer's supply chain risk and assign a threat level, following guidance set forth in Intelligence Community Standard (ICS) 731-02, Supply Chain Threat Assessments, the below Pass/Fail ratings will be applied to determine if the Supply Chain Risk is acceptable to the Government using the following **definitions for each threat level**:

- **Critical** – Information indicates a foreign intelligence entity (FIE) or other adversary is engaged in subversion, exploitation, or sabotage of the acquisition item or service's supply chain, including business practices and relationships. Alternative information indicates a FIE or other adversary has established an overt or clandestine relationship within the supply chain, and that a FIE or other adversary has the capability and intent to engage in subversion, exploitation, or sabotage of the acquisition item or service's supply chain.
- **High** – Information indicates a FIE or other adversary has the capability and intent to engage in subversion, exploitation or sabotage of the acquisition item or service's supply chain; however, there are no indications of subversion, exploitation, or sabotage.
- **Medium** - Information indicates a FIE or other adversary has either the capability or the intent to engage in subversion, exploitation or sabotage of the acquisition item or service's supply chain; however, there are no indications of subversion, exploitation, or sabotage.
- **Low** - Information indicates a FIE or other adversary have neither the capability nor the intent to engage in subversion, exploitation, or sabotage of the acquisition item or service's supply chain.
- **Insufficient Information** – The information available is insufficient to assign a threat level to a FIE's or other adversary's capability and intent to engage in subversion, exploitation, or sabotage of the acquisition item or service's supply chain.

Table M.5 Rating for Supply Chain Risk

Supply Chain Risk Rating	Description
Pass	This Sub-Factor is met when NGA Security determines the Supply Chain Risk is assessed as Medium, Low, or Insufficient Information.
Fail	This Sub-Factor is not met when NGA Security determines the Supply Chain Risk is assessed as Critical or High.

15. Place of Performance

Performance shall take place in a performer facility anywhere in the United States with prior approval by the COR.

16. Period of Performance

Base Phase I: The base period of performance shall be 12 months.

Option Phase II: There will be a go/no-go evaluation at the end of Phase I to determine if a follow-on 12-month Phase II shall occur. Phase II is an option phase.

17. Optional Performance

If NGA determines that the Phase I base period has produced high-quality results and that the overall output of a performer warrants continued support, then NGA may exercise its option for a Phase II. NGA will notify a Phase I performer of either NGA intent to exercise the Phase II option or not to exercise a Phase II option 30 days prior to the end the Phase I base period.

The exercise of any Phase II option will be based on performer achievement, performance, an overall assessment of all Phase I work products, the potential benefits to NGA of those products, and the availability of funding. NGA reserves the right to not execute the Phase II option for any reason whatsoever.

18. Attachments

Attachment #	Name
1	Attachment 1_Topic6_DKTM (Section 6,7,8 Continued) *[File is located on Classified ARC. See Section 5 for instructions on how to get access to the classified ARC.]*
2	DD254
3	Facility Clearance Level template
4	Personnel Security Clearance Level Information template

19. References

1. John A. Volpe National Transportation Systems Center, Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System, 2001.

2. Humphreys, T. E., Ledvina, B. M., Psiake, M. L., et al., *Assessing the spoofing threat: Development of a portable GPS civilian spoofer*, 2008 ION GNSS Conference Savanna, GA, September 16–19, 2008.

Attachment 1

Attachment 1_Topic6_DKTM (Section 6,7,8 Continued)

[File is located on Classified ARC. See Section 5 for instructions on how to get access to the classified ARC.]

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the National Industrial Security Program (NISP) apply to all security aspects of this effort involving classified information.)

OMB No. 0704-0567
OMB approval expires: May 31, 2022

RETURN COMPLETED FORM AS DIRECTED IN THE INSTRUCTIONS.

1. CLEARANCE AND SAFEGUARDING

a. LEVEL OF FACILITY SECURITY CLEARANCE (FCL) REQUIRED *(See Instructions)*
Top Secret

b. LEVEL OF SAFEGUARDING FOR CLASSIFIED INFORMATION/ MATERIAL REQUIRED AT CONTRACTOR FACILITY
None (See instructions)

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable.)*

☐ **a. PRIME CONTRACT NUMBER** *(See instructions.)*

☐ **b. SUBCONTRACT NUMBER**

☒ **c. SOLICITATION OR OTHER NUMBER** **DUE DATE** *(YYYYMMDD)*
HM047622R0008

3. THIS SPECIFICATION IS: *(X and complete as applicable.)*

☒ **a. ORIGINAL** *(Complete date in all cases.)* **DATE** *(YYYYMMDD)* 20211213

☐ **b. REVISED** *(Supersedes all previous specifications.)*
REVISION NO. **DATE** *(YYYYMMDD)*

☐ **c. FINAL** *(Complete Item 5 in all cases.)* **DATE** *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? ☒ No ☐ Yes *If yes, complete the following:*
Classified material received or generated under _____ *(Preceding Contract Number)* **is transferred to this follow-on contract.**

5. IS THIS A FINAL DD FORM 254? ☒ No ☐ Yes *If yes, complete the following:*
In response to the contractor's request dated _____ **, retention of the classified material is authorized for the period of:** _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE(S) (CSO) *(Name, Address, ZIP Code, Telephone required; Email Address optional)*

7. SUBCONTRACTOR(S) *(Click button if you choose to add or list the subcontractors -- but will still require a separate DD Form 254 issued by a prime contractor to each subcontractor)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE(S) (CSO) *(Name, Address, ZIP Code, Telephone required; Email Address optional)*

8. ACTUAL PERFORMANCE *(Click button to add more locations.)*

a. LOCATION(S) *(For actual performance, see instructions.)*	b. CAGE CODE *(If applicable, see Instructions.)*	c. COGNIZANT SECURITY OFFICE(S) (CSO) *(Name, Address, ZIP Code, Telephone required; Email Address optional)*
NATL GEOSPATIAL-INTELLIGENCE AGENCY, 7500 GEOINT DRIVE SPRINGFIELD VA 22150-7500 USA	HM0476	

9. GENERAL UNCLASSIFIED DESCRIPTION OF THIS PROCUREMENT
Detecting Known Trajectory Manipulations (DKTM)

10. CONTRACTOR WILL REQUIRE ACCESS TO: *(X all that apply. Provide details in Blocks 13 or 14 as set forth in the instructions.)*

- ☐ **a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION**
- ☐ **b. RESTRICTED DATA**
- ☐ **c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI)** *(If CNWDI applies, RESTRICTED DATA must also be marked.)*
- ☐ **d. FORMERLY RESTRICTED DATA**
- **e. NATIONAL INTELLIGENCE INFORMATION:**
  - ☒ **(1) Sensitive Compartmented Information (SCI)**
  - ☒ **(2) Non-SCI**
- ☐ **f. SPECIAL ACCESS PROGRAM (SAP) INFORMATION**
- ☒ **g. NORTH ATLANTIC TREATY ORGANIZATION (NATO) INFORMATION**
- ☐ **h. FOREIGN GOVERMENT INFORMATION**
- ☐ **i. ALTERNATIVE COMPENSATORY CONTROL MEASURES (ACCM) INFORMATION**
- ☒ **j. CONTROLLED UNCLASSIFIED INFORMATION (CUI)** *(See instructions.)*
- ☒ **k. OTHER (Specify)** *(See instructions.)*

SEE SECTION 13

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL: *(X all that apply. See instructions. Provide details in Blocks 13 or 14 as set forth in the instructions.)*

- ☒ **a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY** *(Applicable only if there is no access or storage required at contractor facility. See instructions.)*
- ☐ **b. RECEIVE AND STORE CLASSIFIED DOCUMENTS ONLY**
- ☐ **c. RECEIVE, STORE, AND GENERATE CLASSIFIED INFORMATION OR MATERIAL**
- ☐ **d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE**
- ☐ **e. PERFORM SERVICES ONLY**
- ☐ **f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S.,PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES**
- ☐ **g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER**
- ☐ **h. REQUIRE A COMSEC ACCOUNT**
- ☐ **i. HAVE A TEMPEST REQUIREMENT**
- ☒ **j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS**
- ☐ **k. BE AUTHORIZED TO USE DEFENSE COURIER SERVICE**
- ☒ **l. RECEIVE, STORE, OR GENERATE CONTROLLED UNCLASSIFIED INFORMATION (CUI).** *(DoD Components: refer to DoDM 5200.01, Volume 4 only for specific CUI protection requirements. Non-DoD Components: see instructions.)*
- ☒ **m. OTHER (Specify)** *(See instructions.)*

SEE SECTION 13

12. PUBLIC RELEASE

Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the National Industrial Security Program Operating Manual (NISPOM) or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for review and approval prior to release to the appropriate government approval authority identified here with at least office and phone contact information and if available, an e-mail address. *(See instructions)*

☐ **DIRECT** ☒ **THROUGH** *(Specify below)*

Public Release Authority:

SEE SECTION 13

13. SECURITY GUIDANCE

The security classification guidance for classified information needed for this effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended.
(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. The field will expand as text is added. When removing any expanded text area, use delete key or backspace key, then click out of the text field for it to shrink after the text has been deleted. Also allows for up to 6 internal reviewers to digitally sign. See instructions for additional guidance or use of the fillable PDF.)

Questions regarding this solicitation DD 254 should be directed to the Technical POC. Prime contractor will provide copies of subcontractor DD254s to NGA Industrial Security.

CO: Daniela Garavito
COR: Patrick Smith

Accounting for Classified:
As indicated in the 32 CFR part 117, contractors shall establish an information management system to protect and control the classified information in their possession. Contractors shall ensure that classified information in their custody is used or retained only for a lawful and authorized U.S. Government purpose. The U.S. Government reserves the right to retrieve its classified material or to cause appropriate disposition of the material by the contractor. The information management system employed by the contractor shall be capable of facilitating such retrieval and disposition in a reasonable period of time. Authorized NGA personnel may request and receive a listing from the contractor's information system of all classified entrusted to the contractor from NGA or in connection to this contract for NGA.

Authorized personnel consist of NGA program personnel for the contract and personnel from NGA Security. If there is any doubt if the person is authorized access, clarification will be made by Industrial Security or the contracting officer of record.
Retention of classified after the period of performance is only authorized long enough to properly close out the contract and properly dispose of classified as directed by the contracting officer or representative. The manner of disposing of classified shall adhere to the32 CFR part 117. A copy of the certification of disposition by the contractor of government furnished property and information shall be provided to Industrial Security if classified was released to the safekeeping of the contractor.

Classification Guidance:
Specific classification guides for this program will be issued by the program office or COR on this effort directly to the contractor.
With the type of environment NGA operates in, the contractor may be exposed to other NGA programs or classified information not associated with this contract or the information may not be referenced in the program classification guides but may be referenced in the Consolidated NGA Security Classification Guide (CoNGA SCG). The contractor program manager or contractor security office can request access to the guides from the NGA program office who will provide links or soft/hard copies of the requested security guides. The security guides can also be found on JWICS. All classified guides are accountable items and if provided to the contractor shall be tracked and accounted for in the contractor's information management system.

Controlled Unclassified Information:
In accordance with DoD Instruction 5200.48, Controlled Unclassified Information (CUI), CUI information and material may be transmitted via first class mail, parcel post, or, bulk shipments. When practical, CUI information may be transmitted electronically (e.g., data, website, or e-mail), via approved secure communications systems or systems utilizing other protective measures such as Public Key Infrastructure or transport layer security (e.g., https). Avoid wireless telephone transmission of CUI when other options are available. CUI transmission via facsimile machine is permitted; however, the sender is responsible for determining whether appropriate protection will be available at the receiving location before transmission (e.g., facsimile machine attended by a person authorized to receive CUI; facsimile machine located in a controlled government environment).
The absence of the CUI marking on information does not mean the information may be released. Some records may still require protection. The contract will seek further guidance when needed.

E-Nomination Portal:
NGA Contractor SCI nomination process is completed within a web-based portal known as the e-Nomination portal. To gain access to the e-Nomination portal the contractor shall delegate a security professional to make the nominations. The number of personnel assigned to make nominations is limited per the COR For technical issues the contractor will need to contact the e-Nomination support team via e-mail. The following information of the security professional shall be provided to the COR to generate an e-Nomination account.
1. Full Name
2. Primary e-mail address
3. Alternate e-mail address: in case the primary e-mail address holder is not available. It is recommended that this be a group e-mail box or distribution list.
4. Physical Address
Once a nomination is submitted, the e-Nomination portal assigns an e-Nomination Number to the submission. In an effort to provide better OPSEC and protect personal identification information when corresponding via unsecure means (encrypted e-mail authorized) the contractor is not authorized to pair the nominated individual's name with the assigned e-Nomination number. If the contractor misplaces their copy of nomination personnel and e-Nomination numbers list, the contractor security office shall contact the COR for assistance. NGA Industrial Security and NGA Personnel Security may be contacted for assistance if the COR is not available. Only a limited number of personnel in these offices have access to this information and may not be available for assistance at the time of call.

Foreign Travel:
Contractors with SCI access, conducting official or unofficial travel outside the Continental United States shall enter travel details into PeopleSoft 30 days prior to the trip. Upon reentry into the Continental United States, the individual has 10 calendar days to complete post travel forms located in PeopleSoft. If the individual does not have access to PeopleSoft, their information can be entered into PeopleSoft by their COR or FSO (this also applies to the post travel forms).

Government Furnished Property and Information:
If contract personnel are issued a Common Access Card (CAC) the contract personnel will follow the directions of their assigned Trusted Agent for the CAC. When contract personnel depart the contract they will need to notify their assigned Trusted Agent. If the contract personnel will no longer be supporting NGA via an NGA contract the CAC shall be turned in to the NGA Site CAC Office, the Trusted Agent or the COR. If contract personnel are unable to contact the Trusted Agent or return the CAC, it is the contractor security office's responsibility to collect the CAC from the individual and notify and seek further direction from the COR and Industrial Security the same day. Personnel on this contract may be issued other types of government identification or other items (together or separately is referred as items). These items are not limited to but may include the Intelligence Community Access Badge, tokens or NGA Parking Hang Tag. When contract personnel depart the contract, the contracting company must notify the COR, the program office, and Industrial Security. If the contract personnel will no longer be supporting NGA via an NGA contract the items shall be turned into the NGA Workforce Support

Center or the COR. If contract personnel are unable to turn these items in to the Workforce Support Center or COR, it is the contractor security office's responsibility to collect the items from the individual to include completing any debriefing paperwork needed and notify and seek further direction from the COR or Industrial Security. Items shall be returned within 10 business days (timeline may be extended with authorized documented exceptions by NGA Security) to an NGA Site Security office. The contractor shall track and record delivery of items collected and keep the receipts of the returned items for the life of the contract and be able to present them for review if requested by NGA Security Personnel (military/government/contractor). Digitalizing receipts for filing to reduce storage is authorized.

Personnel Security Clearance:
All contractor Single Scope Background Investigation – Periodic Reinvestigation (SSBI-PR) shall be submitted to the Defense Counterintelligence and Security Agency (DCSA) Personnel Security Management Office - Industry (PSMO-I) in a timely manner to prevent interruption of continuous access. When submitting the package, the contractor will ensure the NGA Personnel Security Office address is used in the "Thru Address" block. Also, in the comment section the contractor should place the following statement "For SCI access with NGA". Once the investigation is completed the contractor shall notify NGA Personnel Security that the investigation is in need of adjudication. NGA Personnel Security offers status checks of personnel who have been nominated for SCI access. This is done in two separate methods. One is done monthly and provides an in-depth review. To obtain this service the contractor security office needs to contact personnel security to establish a monthly reoccurring appointment. The other method is via e-mail. The e-mail status check will provide at what stage the nomination is in such as awaiting COR approval, adjudication action or awaiting additional information. The e-mail status is done bi-weekly. The subject of the e-mail shall be "Status Check". Multiple nominations can be checked with one e-mail request however the list of personnel must be placed in an Excel compatible document.
Upon request from NGA, a list of all personnel supporting the contract shall be provided within 24 hours of request unless indicated otherwise.

Protection of Personally Identifiable Information (PII):
All PII information shall be safeguarded in accordance with established law, regulation and polices. The contractor will control all PII information connected to NGA as CUI. NGA defines PII as "Information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc., alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."
A contractor shall report the detection or discovery of suspected or confirmed incidents involving PII to their program manager or COR. If the program manager or COR is unavailable or has a conflict of interest, contact the Privacy Office. The following is a short example list and does not include all that is considered or may be considered PII:

Security Clearance Level
Leave Balances; type of leave used
Family Data
Religion, Race, National Origin
Home Address
Home Telephone Number
Personal E-mail Address
Social Security Number
Biometric Identification (such as fingerprints)
Date of Birth
Place of Birth
Mother's Maiden Name
Performance Ratings
Participants Names/Results in NGA Courses
Alien Registration Number
Driver's License Number
Medical or Financial Records

Protection of Unclassified Information:
The Contractor shall not release outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless the Contracting Officer has given prior written approval or in performance of a project that has been scoped and negotiated by NGA with the contractor. Release and disclosure guidance provided to subcontractors shall be "all release and disclosure request shall be submitted through the prime contractor to NGA".
CUI is unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. Per NGAI 5200.1, Information Security, Enclosure 15, The primary categories of CUI created by NGA are FOR OFFICIAL USE ONLY (FOUO) and LIMITED DISTRIBUTION (LIMDIS).
NGA uses FOUO to designate CUI that falls under one of the Freedom of Information Act Exemptions, 2 through 9 that can be found in Enclosure 3, Appendix 1 of NGA Instruction 5750.1 Freedom of Information Act / Privacy Act Requests / Mandatory Declassification Review Program. Information that is on the NGA OPSEC Program Critical Information List that can be found in Enclosure 8 of NGA

Instruction 5200.4, Operations Security. Information that is determined to be FOUO, regardless of medium, is indicated by the appropriate markings as provided. In general, markings on an FOUO document indicate the originating agency/office, banner line markings, and portion markings. NGA will continue to utilize the FOUO marking until the Office of the Director of National Intelligence (ODNI) provides further marking guidance to the Intelligence Community.

Public Release:
Unless noted in the contract or FAR, release request of contract information shall be routed to the Contracting Officer by the way of the NGA program office for this contract and/or task orders. Request to release information (classified or unclassified) to international partners requires approval from NGA's Office of International Affairs.

Security Incident Reporting:
In addition to 32 CFR part 117 requirements, contractors shall report all security incidents, infractions and any other situation if it involves the possibility of unauthorized release or disclosure of classified information to include incidents that jeopardizes classified information. This includes FGI and NATO classified information. Notification recipients shall include the DCSA IS Rep for the company, NGA Industrial Security, NGA Investigations Division, NGA continuous Evaluation Unit (CEU) and the Initial notification will consist of only the following information via e-mail of the day of discovery:

Incident type
Personnel Involved
Contract Number
Primary COR
Task Order COR
Date and Time of Incident
Lead Company Investigator for the Incident
Estimated Date of Completion of Investigation
Incident information can elevate to the level of classified. Be cognizant of the data and the classification level of the report. of. The investigation incident report shall be transmitted to NGA Investigation Division (for government investigation and determination), NGA Industrial Security (to ensure compliance), and the CORs for the base contract (number located on the DD 254) and the task order contract (if applicable) for contract monitoring. The report will be transmitted by the most secure means possible in this order; classified e-mail to all listed parties. If classified e-mail is not an option transmit via secure fax to NGA Industrial Security for distribution. If secure FAX is not an option, transportation between the company's registry and NGA registry (mail/FedEx) is authorized. Only as a last resort should the investigation report be hand carried to Industrial Security for distribution. If AIS equipment is involved it is the contractor's responsibility to have the AIS equipment properly transported (such as courier authorization) to an NGA facility for investigation, if requested by NGA.

Subcontracting requirement:
All subcontracts requiring access to classified information require CO/COR approval. Once submitted for approval an e-mail notification shall be sent to Industrial Security and the contract program office. Subcontracts not requiring access to classified information still require the contract program office approval. The prime contractor shall certify their proposed subcontractor is not effectively owned or controlled by a foreign interest or cleared under a Special Security Agreement (SSA). This validation will be through the Defense Counterintelligence and Security Agency. Access to proscribed information by a company cleared under an SSA may require NGA to complete a National Interest Determination (NID) to determine if release of proscribed information to the subcontractor is in the best interest of national security. The subcontractor personnel will not be nominated for or given access to classified information until the NID is validated by NGA Industrial Security.

Industrial Security Branch Support:
NGA is responsible for all SCI connected to this contract. To assist and provide proper oversight to the contractor, NGA will conduct visits to the contractor sites. These visits (commonly known as Customer Assistance Visits or CAVs) will range from 1 NGA Industrial Security person (who may be military, government, or contractor for security services to NGA) or a team of personnel to provide guidance and assistance in protection of national security information. Other government organization may be invited to attend or be notified of such visits and the results of such visits. There may be other visits (announced and unannounced) to ensure compliance of other security and non-security related requirements. The contractor security professional responsible for the contract will contact NGA Industrial Security to coordinate the CAV annually. Initially, all physical security requirements connected to ICD 705 will be coordinated through NGA Industrial Security. The NGA Classification Guide provides general classification guidance when dealing with safeguarding SCI. Per ICD 705-2, if a SCIF conference room (accredited under this contract) will be used by another organization (when a Co-utilization/Joint Utilization is not in place or being coordinated) the contractor shall notify Industrial Security via e-mail within 10 days. It is understood at times meetings are scheduled within the 10-day window, in this case immediate notification is required.
If requested NGA Industrial Security will provide a limited supply of physical and digital copies or training aids and reference material such as the NISPOM, ICD 705,

Inspection Reporting:
Contractor is responsible to submit the following Defense Counterintelligence and Security Agency documents to the NGA Industrial Security Branch within 30 days of completion or upon request prior to an NGA Industrial Security Customer Assistance Visit:
• DCSA Results Letter
• Rating Matrix
• List of Vulnerabilities, observations, recommendations, and other documentation provided by DCSA following an inspection

Ref 10e1: SCI Access required. No public release of information authorized, public disclosure or confirmation of any subject related to the support contract is not authorized without first obtaining written approval from the GCA.

Ref 10e2: Non-SCI Information is not releasable to contractor employees who have not received a clearance at the appropriate security level. Written concurrence of the GCA is required prior to subcontracting. Access to Intelligence information required for performance.

Ref 10g: NATO: During this contract, the contractor will have access to NATO Information. Upon approval from NGA, the contractor will be indoctrinated at the appropriate access level. Per the NISPOM, contractors are required to have annual NATO refresher training.

Ref 10j: For Official Use Only (FOUO) Information generated and/or provided under this contract shall be safeguarded and marked as specified in NGAI 5200.1.

Ref 11a: Contractor performance is restricted to locations identified in Block 13. Government agency or activity will provide security classification guidance for performance of this contract.

Ref 11j : OPSEC:
NGA applies strong OPSEC measures to deny potential adversaries access to NGA's critical information. To ensure the continuation of denial, personnel assigned to this contract shall comply and support the OPSEC plans associated with this contract. The contractor shall remain compliant with NGA OPSEC training requirements. If warranted, the contractor will work with the OPSEC Program Management or the Key Component OPSEC Officer to protect NGA's critical information.

Ref 11l: RECEIVE, STORE OR GENERATE CONTROLLED UNCLASSIFED INFORMATION (CUI): (DoD Components: refer to DoDI 5200.48 for specific CUI protection requirements. Non-DoD Components: see instructions.)

[Block: 8]
[Location] NATL GEOSPATIAL-INTELLIGENCE AGENCY, 3838 VOGEL ROAD
ARNOLD MO 63010-6238
USA [Location Code] HM1575
[Location] NATL GEOSPATIAL-INTELLIGENCE AGENCY, 3200 SOUTH SECOND STREET
ST. LOUIS MO 63118
USA [Location Code] HM1575

[Block: 12]
DoDAAC[HM0476] Release Information[SEE SECTION 13]
Location Code/Agency Name/Address[HM0476, ATTN: MS S84 - OCS
ATTN: MS S84 - OCS, NGA SPRINGFIELD 7500 GEOINT DRIVE SPRINGFIELD VA 22150-7500, SPRINGFIELD, VA, 22150-7500, USA]

List of Attachments (All Files Must be attached Prior to Signing, i.e., for any digital signature on the form)

NAME & TITLE OF REVIEWING OFFICIAL	SIGNATURE
JAMIE MONGOLD REGIONAL SECURITY OFFICER	MONGOLD.JAMIE.LEE.1256336320 Digitally signed by MONGOLD.JAMIE.LEE.1256336320 Date: 2021.12.16 09:22:40 -05'00'

14. ADDITIONAL SECURITY REQUIREMENTS

Requirements, in addition to NISPOM requirements for classified information, are established for this contract.

☐ No ☒ Yes *If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the CSO. The field will expand as text is added or you can also use item 13. When removing any expanded text area, use delete key or backspace key, then click out of the text field for it to shrink after the text has been deleted. (See instructions for additional guidance or use of the fillable PDF.)*

SEE SECTION 13

15. INSPECTIONS

Elements of this contract are outside the inspection responsibility of the CSO.

☐ No ☒ Yes *If Yes, explain and identify specific areas and government activity responsible for inspections. The field will expand as text is added or you can also use item 13. When removing any expanded text area, use delete key or backspace key, then click out of the text field for it to shrink after the text has been deleted. (See instructions for additional guidance or use of the fillable PDF.)*

NGA IS RESPONSIBLE FOR OVERSIGHT OF SCI

16. GOVERNMENT CONTRACTING ACTIVITY (GCA) AND POINT OF CONTACT (POC)

a. GCA NAME	c. ADDRESS *(Include ZIP Code)*	d. POC NAME
NGA	7500 GEOINT DR. SPRINGFIELD VA 22150	NGA INDUSTRIAL SECURITY
		e. POC TELEPHONE *(Include Area Code)* +1 (571) 557-3355
b. ACTIVITY ADDRESS CODE (AAC) OF THE CONTRACTING OFFICE *(See Instructions)* HM0476		f. EMAIL ADDRESS *(See Instructions)*

17. CERTIFICATION AND SIGNATURES

Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below. Upon digitally signing Item 17h, no changes can be made as the form will be locked.

a. TYPED NAME OF CERTIFYING OFFICIAL *(Last, First, Middle Initial)* *(See Instructions)*	d. AAC OF THE CONTRACTING OFFICE *(See Instructions)*	h. SIGNATURE
MAURICE WILLIAMS	HM0476	WILLIAMS.MAURICE.1181271198 Digitally signed by WILLIAMS.MAURICE.1181271198 Date: 2021.12.16 13:33:18 -05'00'
b. TITLE INDUSTRIAL SECURITY LEAD	e. CAGE CODE OF THE PRIME CONTRACTOR *(See Instructions.)*	
c. ADDRESS *(Include ZIP Code)* 7500 GEOINT DR. SPRINGFIELD VA 22150	f. TELEPHONE *(Include Area Code)* +1 (571) 557-8440	i. DATE SIGNED *(See Instructions)* 20211216
	g. EMAIL ADDRESS *(See Instructions)*	

18. REQUIRED DISTRIBUTION BY THE CERTIFYING OFFICIAL

☐ a. CONTRACTOR

☐ b. SUBCONTRACTOR

☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR

☐ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION

☒ e. ADMINISTRATIVE CONTRACTING OFFICER

☒ f. OTHER AS NECESSARY *(If more room is needed, continue in Item 13 or on additional page if necessary.)*

INDUSTRIALSECURITY@NGA.MIL

SOURCE SELECTION INFORMATION – SEE FAR 2.101 & 3.104

Facility Security Clearance Level and Foreign Ownership, Control, or Influence Information (Template)

Company Name	Street	City	State	Zip Code	CAGE Code	FCL	Safeguarding Capability	Comment
ABC Company						Top Secret	Secret	
XYZ Company						Top Secret	Top Secret	

Note: This document contains personally identifiable information and is for official use only. Unauthorized dissemination or use of personally identifiable information is a violation of Federal law. Individuals in violation may be subject to fines, disciplinary actions or both (P.L. 93-579).

SOURCE SELECTION INFORMATION – SEE FAR 2.101 & 3.104

Personnel Security Clearance Information (Template)

Full Name (Last, First Middle)	Current Employer	DOB	POB	SSN	Type of Investigation / Date		SCI Eligibility Date	Status of SCI	Govt. Sponsor
YYYYYY, Jane Ann	XYZ Company	05/06/1970	Washington, DC	666-66-2345	SSBI-PR	01/20/2009	01/25/2009	Briefed	DIA
XXXXX, John Henry	BBB Company	02/01/1981	San Diego, CA	777-77-7890	SSBI	07/26/2001	08/30/2011	Debriefed	NGA

Note: This document contains personally identifiable information and is for official use only. Unauthorized dissemination or use of personally identifiable information is a violation of Federal law. Individuals in violation may be subject to fines, disciplinary actions or both (P.L. 93-579)