RFQ ATTACHMENT A
PERFORMANCE WORK STATEMENT (PWS)

Title: Supply Chain Risk Illumination Professional Services and Tools (SCRIPT) Blanket Purchase Agreement (BPA)

1. Purpose:
The U.S. Government has a requirement to establish core, multi-component, supply chain risk illumination tools with the ability to identify self-attested, public, as well as, purchased data, in real time, along with a persistent monitoring capability. The delivery of these capabilities, and associated data analyses, are required in order to provide supplier and network assessment services to Department of Defense (DoD) and Federal Civilian Executive Branch (FCEB) Agencies that have shared mission areas. This requirement will foster a whole of government (WoG) approach to assess risk across the federal supply chain and to further mitigate vendor threats. This capability will become an open resource based on security classification of analyzed data for potential use within the spectrum of information security environments (e.g. TS-SCI, Secret, and CUI levels) within the DoD and other government agencies.

The availability of supply chain risk illumination tools and analytic support services provides capabilities in accordance with the following Executive Orders, Public Laws and other current and future legislation, policy, directives, and regulations as it applies to industrial base and supply chain risk management and resiliency:

- EO 13806 Assessing and Strengthening Manufacturing and Defense Industrial Base and Supply Resiliency
- EO 13817 Threat to the Domestic Supply Chain from Reliance on Critical Minerals
- EO 13873 Securing the ICT and Services Supply Chain
- EO 14017 America's Supply Chains
- EO 14028 Improving the Nation's Cybersecurity,
- Public Law 116-92 FY 2020 NDAA Section 845
- Public Law 113-291 FY2015 NDAA Sections 841-843, as amended by Public Law 116-92 FY2020 NDAA Section 822
- Public Law 115-91 FY2018 NDAA Section 1643
- Public Law 105-261 FY1999 NDAA Section 1237
- Public Law 116-283 FY2019 NDAA Section 889,
- Title 10, USC Section 2339a, (Requirements for information relating to supply chain risk)
- Title 41 USC Section 4713 (Authorities relating to mitigating supply chain risks in the procurement of covered articles)
- Department of Defense Instruction (DoDI) 4140.01 (DoD Supply Chain Materiel Management Policy) (current dated version)
- DoDI 5200.44 (Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)) Incorporating Change 3, (or current dated Change revision)
- DoDI 5000.83 (Technology and Program Protection to Maintain Technological Advantage); (current dated Change revision)
- DoDI 5000.85 (Major Capability Acquisition); Incorporating Change 1, (or current dated Change revision)

- DoDI 5000.90 (Cybersecurity for Acquisition Decisions and Program Managers) (current revision)
- DoDI 5000.91 (Product Support Management for the Adaptive Acquisition Framework); (current revision)
- Directive-Type Memorandum 18-003 (Prohibition on Providing Funds to the Enemy and Authorization of Additional Access to Records); June 8, 2020.
- Army Regulation 70-77 (Program Protection); 8 June 2018
- OMB Memorandum M-23-03, Guidance on Federal Information Security and Privacy Management Requirements
- OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

2. Background:
The Office of the Under Secretary of Defense (OUSD) Acquisition and Sustainment (A&S), in support of Department of Defense (DoD) Service Components and 4th Estate Agencies, as strategic stakeholders, have a requirement to identify and manage risk and supply chain vulnerabilities within the Defense Industrial Base (DIB) and domestic Commercial Information Technology marketplace. The critical informational needs are required in support of areas such as: Research and Engineering technology development, cyber security of hardware and software, manufacturing, acquisition, sustainment, contractor support to operations, infrastructure, intelligence and counterintelligence, and telecommunication services. OUSD (A&S) is responsible for assessing and monitoring the industrial health and security of the DIB as well as those industrial sectors that are inextricably linked to the resiliency and effectiveness of the DIB. Defense Production Act (DPA) Title III designates supply chain illumination as a critical requirement enabling the identification of: opportunities, vulnerabilities, and systemic dependencies that are crucial to assessing risk. Additionally, the DPA of 1950 confers upon the Federal Government a broad set of authorities to influence domestic industry in the interest of national defense, enhance and support domestic preparedness, response, and recovery from natural hazards, terrorist attacks, or other national emergencies. The authorities can be used across the Federal Government to shape the DIB so that, when called upon, it can provide essential materials and goods needed for this purpose. DPA authorizes the Federal Government, in part, to require persons (including businesses and corporations) to prioritize, accept contracts for materials and services as necessary to promote national defense, expand productive capacity and supply, as well as incentivize the DIB to expand the production and supply of critical materials and goods.

The current business operating environment presents several Supply Chain Risk Management (SCRM) challenges: (1) reliance on commercial services and technologies and multiple tiers of the global DIB that shift at an increasingly fast rate, and; (2) vast availability of commercial items and services through simplified acquisitions and/or purchase cards that may not have been fully vetted for cyber and supply chain risk. Recent events affecting the global industrial base have increased the urgency of SCRM being implemented and executed in support of National Security Systems (under 10 USC Section 2339a) for DoD systems and networks, and in support

of the Federal Acquisition Security Council (FASC)[1] established under the SECURE Technology Act, and 41 USC Sections 1326[2] and 4713[3] and Executive Orders 14017 and 14028.

Additionally, OUSD (A&S) Industrial Policy (INDPOL) is heavily involved in the review of DoD-nexus Committee on Foreign Investment in the United States (CFIUS). INDPOL plays a vital role in reviewing potential problems related to foreign investment in U.S. companies. INDPOL reviews global market activity in the defense sector to determine if there are any potential impacts to the U.S. defense industrial base. These findings are used to determine whether a CFIUS review is warranted. The Foreign Investment Risk Review Modernization Act was passed last year, and it expands CFIUS' jurisdiction considerably. The CFIUS mission spans across the Federal Government including the Intelligence Community, and analysis associated with CFIUS reviews are necessarily shared across all agencies.

In 2018, Congress passed Title II of the SECURE Technology Act, the Federal Acquisition Supply Chain Security act of 2018, which created the Federal Acquisition Security Council (FASC). The FASC focuses specifically on the Information and communications technology (ICT) sectors (functional crosscut of the 16 critical infrastructure sectors). The Council assists departments and agencies in: (1) determining the risk to the ICT supply chain: (2) disseminating supply chain risk information, and; (3) deciding what actions to take to mitigate the risk. Each department and agency will be required to have a SCRM program that meets the FASC developed criteria. In addition to developing uniform criteria for supply chain risk management, the FASC can make specific recommendations for mitigations to address risky vendors, including the exclusion of such vendors from the ICT supply chain. OUSD (A&S) provides leadership to the FASC and works closely with the Department of Homeland Security, Cybersecurity, and Infrastructure Security Agency (DHS CISA) and other Federal Agencies such as the Department of Energy (DOE) to enhance protection of the DIB and other critical infrastructure sectors. As stated in the 2021 Executive Order 14017, America's Supply Chains require a resilient, diverse, and secure supply chain to ensure our economic prosperity and national security. Resilient American supply chains will revitalize and rebuild domestic manufacturing capacity, maintain America's competitive edge in research and development, and create well-paying jobs.

As a result, the GSA Schedules program intends to issue a Multiple Award BPA for Information Technology (IT) subscription-based supply chain risk assessment analytic tools and associated professional support services. Direct OUSD (A&S) customer feedback was used to develop this integrated capability approach to provide access to a suite of supply chain illumination tool capabilities. With this approach the OUSD (A&S) leadership has indicated that a GSA SCRM

[1] Public Law 115-390 Dec.21, 2018, SEC 202 FEDERAL ACQUISITION SUPPLY CHAIN SECURITY. Established the Federal Acquisition Security Council, which among other responsibilities and authorities requires assessment of supply chain risk to include Exclusion and Removal Orders. https://www.congress.gov/115/plaws/publ390/PLAW-115publ390.pdf

[2] The head of each executive agency shall be responsible for—
(1) assessing the supply chain risk posed by the acquisition and use of covered articles and avoiding, mitigating, accepting, or transferring that risk, as appropriate and consistent with the standards, guidelines, and practices identified by the Council under section 1323(a)(1) and
(2) prioritizing supply chain risk assessments conducted under paragraph (1) based on the criticality of the mission, system, component, service, or asset. https://www.law.cornell.edu/uscode/text/41/1326

[3] https://www.law.cornell.edu/uscode/text/41/4713

Illumination Tools BPA would be considered a preferred use vehicle for the DoD, its Component Services, and the 4th Estate enterprise. Use of Multiple Award Schedule (MAS) BPAs eliminates contracting and open market costs such as: the search for sources; and the development of technical documents and solicitations. These BPAs will further decrease costs, reduce paperwork and save time by eliminating the need for repetitive, individual purchases from the GSA Schedule contract. The end result is a purchasing mechanism for the Government that works better and costs less.

3. Objective/Scope:

In accordance with the Federal Acquisition Streamlining Act of 1994, the OUSD (A&S) office has a requirement to acquire access to services and support for the implementation, configuration, maintenance, and delivery of capabilities to provide supplier and network assessment services to DoD and other Federal Agencies that have shared mission areas with DoD. The acquisition of deployable supply chain illumination capabilities for cyber hygiene, supply chain, foreign ownership, control, and influence, vendor vetting and affiliated entity, as well as personnel vetting will enable the government to be continuously and dynamically informed on industry supplier health. This requirement will allow the DoD to holistically screen and vet vendors and underlying supplier networks/affiliated personnel to ensure suppliers are reputable, in good-standing, financially and operationally secure, and will not introduce unacceptable risk to the Government.

This proposed GSA MAS BPA, developed in accordance with FAR 8.405-3 procedures, will allow multiple DoD components and Federal agencies unfettered access to best in class capabilities, enable efficient information sharing and collaboration in support of Federal law and Presidential Executive Orders, and provide best value pricing options. The SCRM Illumination Tool BPA will provide a total solution approach to leverage commercial industry tools, global database resources, and technical analytic support services with prompt, cost-effective delivery, while capturing economies of scale, and while fostering small business markets for sustainable technologies. The North American Industry Classification System (NAICS) codes considered for this requirement are:

- 541519 - Other Computer Related Services,
- 541611 - Administrative Management and General Management Consulting Services, and
- 519290 - Web Search Portals and All Other Information Services.

The corresponding FY23 small business size standards are $34 million and 1,000 employees respectively for this acquisition. The corresponding GSA Schedules Special Item Numbers (SINs) associated with this procurement include:

- SIN 518210C Cloud and Cloud-Related IT Professional Services
- SIN 54151ECOM Electronic Commerce and Subscription Services

- SIN 54151S Information Technology Professional Services
- SIN 541614SVC Supply and Value Chain Management
- SIN 541990RISK, Risk Assessment and Mitigation Services
- SIN 541611 Management and Financial Consulting, Acquisition and Grants Management Support, and Business Program and Project Management Services

4. Tasks

These requirements are intended to provide DoD and affiliated Federal agencies with supply chain tools and analyses of the DIB and other sector supplier networks to include: both private and publicly held companies, along with single network illuminations on affiliated companies and personnel. This requirement is further intended to provide DoD and affiliated Federal agencies with capabilities for automated vendor vetting, supply chain vendor vetting, and affiliated entity vetting to inform supplier health in a continuous and dynamic manner.

4.1 DoD and Federal agencies require the following capabilities:

A. Increased end-to-end transparency and knowledge of multi-tier supply chain ecosystem(s).

B. An understanding of the complex connections and dependencies across specific supply chain ecosystems.

C. Ability to answer complex risk and resiliency questions impacting suppliers across their ecosystem.

D. Continuous discovery and monitoring of dynamic supply chains for indicators of risks to/from individual suppliers and/or specific parts or products.

E. Supply chain ecosystem Maps, Supplier Insights, Risk Scores, Dashboarding Capability, Continuous Monitoring.

F. Industry support networks associated with the end-to-end product lifecycle for information communication technology (ICT), ICT services and solutions.

G. Products must have an Application Programming Interface (API) capability for interoperability with other federal government cloud capabilities.

H. If required, for a cloud service delivery model offering, Federal Risk and Authorization Management Program (FedRAMP) authorized at equivalent DoD Impact Level (IL2, IL4) and Intelligence Oversight compliant within 90 days of contract award, and plans to achieve IL6 with government sponsorship within one calendar year after award.

4.2. For any supply chain/market/industrial base or critical infrastructure sectors requested for further detail illumination, the contractor shall identify and deliver to the Government, all government defined relevant data, in addition to, conducting risk analyses on supply chains, third-party vendors, ultimate beneficial ownership, and financial and operational health within (30) days.

4.3. The contractor may be required to conduct up to (6) in depth data analysis program/product/component/ technology sector/critical infrastructure reviews per quarter each fiscal year. Unless otherwise specified, or instructed, each review, depending on complexity and scale, shall be completed and available via a transferrable medium/format (memorandum, presentation, report, etc.) and/or via a web-accessible dashboard, with the ability to drill down to individual entity data. All underlying risk data shall also be made available in commonly ingestible format (e.g. x.json) via either API or static downloads. The deliverable timelines for reports will be defined at the customer task award level.

4.4. The contractor shall assemble publicly available data on company financials, board governance, demographics (employees, locations, leadership), cyber hygiene/security, all data pertaining to foreign ownership, control, and influence (FOCI).

4.5. The contractor shall classify both public and private companies according to multiple industry classifications including, but not limited to: PSC, UEI, GICS, SIC, and NAICS codes using software and analytics. The contractor shall seamlessly integrate data on private sector operations with known federal government contracting performance information in databases such as CPARS and Supplier Performance Risk System (SPRS).

4.6. The contractor shall provide a structured dataset to support additional processing and risk analysis. Standardized indicators and metrics for material and derogatory information should include, but not be limited to: publicly available information related to criminal proceedings, civil offenses, reputation / brand issues.

4.7. The contractor shall have the technical expertise and demonstrated knowledge to interpret a diverse set of technologies across the following industries: Pharmaceuticals, Aerospace & Defense, Electrical Equipment, Semiconductors, Biotechnology, Contracted Services, Information Technology, Communications and Electronic Equipment, Instruments & Components.

4.8. The contractor shall define system capabilities relevant to frequency of informational updates and monitoring of supply chain/market/industrial base illuminations upon request; specifically, the ability to monitor unstructured open web content.

4.9. The contractor shall leverage industry leading commercial data tools and applications, such as cloud-based tools, data visualization, Natural Language Processing (NLP)/Neural Networks, and open source development tools such as ‘R’ and Python. The contractor shall ensure continued availability through operations and maintenance support, providing all necessary activities to sustain a cloud-based or on-premise operating environment for the data pipeline, master dataset, and analytic application, including, but not limited to the operations in this section.

4.10. The contractor shall be able to access premium commercial data sets to include, but not limited to: News Media, Public Company Data, Private Company Data, Patents, Social Media,

open web, open government (global), global watch list, non-traditional data sources, while obfuscating/anonymizing search and aggregation techniques, with the ability for growth or expansion if other data sets are required.

4.11. The contractor shall leverage technical capabilities that ingest commercially-available information (CAI), publicly-available information (PAI), proprietary data, and government-furnished data sources to populate computational representations of supply chains by drawing on both structured and unstructured data types.
The platform should leverage AI/ML to perform entity resolution and risk analysis, be able to perform language translations, and deliver content in consumable data file structure for government supply chain risk illumination.

4.12. The contractor shall be able to provide executive summaries, reports, and data visualizations to enable decision making through the use of recognized platforms such as briefings, reports, dynamic dashboards, etc.

4.13. The contractor shall have experience working with unstructured data and conducting research and analysis of open source or publicly available data for commercial organizations.

4.14. The contractor shall provide access to a web-based data analytics platform for the performance of supply chain risk analysis, risk identification and reporting, and continuous monitoring.

4.15. The contractor shall train government personnel and the contract shall immediately provide access to begin utilizing the supply chain illumination platform to conduct supply chain risk analysis on entities identified by the government and notify the department or agencies of all relevant industrial health risk indicators/categories supported by the platform.

4.15.1 The platform shall provide business intelligence analytics that address the following **Minimum Risk Indicators /Categories for SCRIPTS Small Business (see Attachment 1)**;

SCRIPTS Small Business *(Set-Aside for Small Business Only)*

1. Financial
2. Foreign Ownership Control or Influence (FOCI)
3. Political and Regulatory
4. Compliance
5. Technology and Cybersecurity

The tools should have the ability to expand or adapt as other health risk indicators/categories are prioritized or identified by the government (e.g.Product Quality/Design, Manufacturing and Supply, Transportation and Distribution, Environment). Any additional risk categories above the minimum elements that Small Business tool providers can meet would be viewed more favorably.

4.15.2 The platform shall provide business intelligence analytics that address the following **Minimum Risk Indicators /Categories for SCRIPTS Unrestricted (see Attachment 1)**;

SCRIPTS Unrestricted - Required Minimum Risk Indicators/Categories:

1. Financial
2. Foreign Ownership Control or Influence (FOCI)
3. Political and Regulatory
4. Compliance
5. Technology and Cybersecurity
6. Manufacturing and Supply
7. Transportation and Distribution
8. Product Quality/Design

Any additional risk categories above the minimum elements that Unrestricted group tool providers can meet would be viewed more favorably.

Additional amplification at the risk sub-category level must include the Minimum Elements to meet identified FAR and program requirements (see Attachment 2).

The platform should have the ability to expand or adapt as other health risk indicators/categories are prioritized or identified by the government (e.g. Product Quality/Design, Manufacturing and Supply, Transportation and Distribution, Environment).

4.16. The contractor shall provide access to the platform for authorized users to run searches on vendors, suppliers, and key personnel based upon defined customer task award quantities and frequency.

4.17. The contractor shall ensure the platform can perform batch uploading of companies, cage codes, UEI, NIINs, etc. and associated personnel/suppliers being screened and vetted for the government.

4.18. The platform must be able to identify companies with any foreign ownership, control, and influence (FOCI) concerns to include: adversarial finance risk indicators, and be able to vet and continuously monitor foreign personnel to identify potential FOCI risk.

4.19. The contractor shall provide access to their supply chain illumination tool database environment, whether through subscription access or cloud-based application services, where applicable, for the term of 12 months. The government will be responsible for renewing subscription-based services access during the defined period of performance. The database environment must also include the ability to access data owned by DoD on any corporate entities, as required.

4.20. The platform must perform automated language translation in the search process to enable identification of potential foreign risk indicators including foreign ownership, control, and influence.

4.21. The contractor shall provide a program management plan as part of the solicitation. The contractor shall support a contract kick-off meeting with all key stakeholders within 15 days after contract award. The contractor shall provide quarterly status reports for all completed and in-progress actions.

4.22. If required by the ordering agency at the task order level, the contractor shall have the capability to provide appropriately cleared technical data analyst support in secure operating environments, up to TS/SCI environment, to assist with requirements collection, rapid payload development, reporting deliverables, training, and quick-turn RFIs.

4.23. The platform shall support reviews of potential foreign acquirers or investors involved in capital and capability provider applications, and those included in CFIUS cases, as appropriate to government agencies.

4.24. The platform shall provide visualization of an entity centric model that displays an expandable view of holistic supplier, vendor, investor, and key management personnel relationships.

4.25. **Continuous Monitoring**

4.25.1. The platform shall be able to continuously monitor for risks to supply availability, or production shortages within supply chains with access to all entities in which supply chain risk analysis is requested.

4.25.2. The platform shall establish or provide flagging mechanisms to alert government points of contact to monitoring events on entities as defined by the government.

4.25.3. The contractor shall include support for platform updates and data management, as part of the subscription agreement, as they become available during the period of performance.

4.26. Deliver a Common Operating Picture

4.26.1. The platform shall deliver self-service dashboarding and visualization tools to provide common operating picture, strategic insights, and inform operational decisions on risk trends across all entities.

4.26.2. The contractor shall create an integrated capability to correlate government derived data and Publicly Available Electronic Information (PAEI) data with Cyber Threat Data to visualize and support a common operating picture.

4.26.3. The contractor shall partner with Joint Cyber Intelligence Tool Suite (JCITS) program leads, and associated vendors/systems as identified by the government to integrate all cyber and non-cyber vulnerabilities.

4.27. **Training**

4.27.1. The contractor shall develop and execute a detailed training plan for government designated users.

4.27.2. The contractor shall provide web-based training to government designated users, as part of its subscription access, for any aspect of the platform, to include one-on-one and team training events as required and defined at the task order level.

4.28. Risk Illumination of Affiliated Entities and Suppliers

4.28.1. The platform shall provide automated supply chain risk analysis research for corporate network illumination and screening of individuals and businesses affiliated with entities designated by government programs as required based on logic provided by program "IF – THEN" statements. (i.e. If an investor or limited partner is from the Cayman Islands then conduct an additional search to determine Ultimate Beneficial Owner). Government programs will supply clear criteria prior to execution of the task order award.

4.28.2. The platform shall enable development of customizable risk scoring with a learning algorithm that can be tuned by government users to better highlight existing or developing risk.

4.29. Continued configuration / tailoring with new sources and risk events

4.29.1. The contractor should offer new development features (i.e. data sources, risk algorithms, user interface changes) as agreed to in the task order by the contractor and the Government. If required by DoD customer(s), the contractor will collaborate with the government to make the dataset broadly available to DoD customers via the DoD Advanced Analytics (ADVANA) enterprise data catalog.

4.30. FedRAMP Authorization (SaaS offering). The contractor will provide available FedRAMP authorization(s) that have been granted for the platform application or hosted environment in support of ordering agency requirements. If not available, the contractor should submit a FedRAMP Initiation Request, with federal agency sponsorship, as required by the ordering agency, to accelerate insights into potential risks associated with government suppliers. The threshold authorization could be at IL4 or FedRAMP HIGH if supporting Controlled Unclassified Information with an objective threshold of IL6 authorization, if required for use in a government secure operating environment. If required by the ordering agency, the contractor shall ensure that all required authority to operate documentation is also provided.

4.31. General

4.31.1. The contractor shall provide data analyst support, at the ordering agency

task order level, to optimize AI system performance as defined at the government task order level.

4.31.2. The contractor shall provide configurable out-of-the-box artificial intelligence (AI), Machine Learning (ML) and NLP models that can adapt to the needs and can be tuned to identify network relationships of Key management personnel, supplier and customer relationships and entity resolution to identify ultimate beneficial ownership (UBO). Additionally, the contractor shall incorporate key aspects of Anti-Money Laundering data, including Crypto currency transactions, to identify sources of funds for entities.

4.31.3. The contractor shall provide dedicated SCRM personnel support for the customer for specific programs or organizations, as defined and requested at the task order level. The requested personnel resources will be dedicated to the organization for the level of effort (hours/dollars) contractually agreed upon and may be virtual or onsite.

4.31.3.1. The contractor shall be responsible for promoting the data on corporations specified by the department, service, or agency to ensure data accuracy.

4.31.3.2. The contractor shall be capable of supporting the customer with surge technical support for SCRM data analysis. This includes creating additional detailed reports as specified by the department, service or agency and is specified as a level of effort (hours/dollars) contractually agreed upon for each type of report.

4.31.3.3. The contractor shall support the department, service, or agency in developing and presenting risk data and reports to provide security council and senior leadership insight into the level of risk that the corporations pose to the DoD and Federal agencies.

4.31.4. Commercial entities information that is procured and input into the enterprise level tool (corporate, personnel profiles) from any agency shall be viewable in the defined database environment or otherwise accessible for sharing with other government agencies for that point in time data pull, at no extra cost to the government (“buy once, share everywhere”). This applies to the corporate and personnel data pulls, as well as to any lower level in depth reports paid for by a government agency. The ability to share this critical Supply Chain Risk information among government agencies requiring government rights in technical data, as described in FAR 52.227-14 for federal agencies and DFARS 252.227-7015 for DoD agencies, is a foundational requirement to support Federal Acquisition Security Council (FASC) strategic objectives, Executive Orders, and Federal/DoD policies.

4.31.5. Annual Report. The contractor shall deliver an Annual Report outlining all accomplished tasks on an annual basis prior to the anniversary of contract award. The report shall be in Microsoft Word electronic format.

4.31.6. Quarterly Program Status Report. The contractor shall deliver quarterly status reports no later than the 10th day of the third month following the previous quarters

closing. The report shall be in Microsoft Word electronic format.

The quarterly report shall include:

- A statement of the period covered (e.g., calendar month, three month period); The period covered by the report shall correspond to one of more invoices.
- Invoiced activities and deliverables in process and completed
- Status of Cyber Hardening activities
- Schedule /spend plan update
- Meetings and briefings attended
- Project status
- Planned activities for the following month
- Activities funded and date funded
- Cost and fee for the reporting period

4.31.7. Performance Requirements (Notional)

Requirements	Performance Standards	Acceptable Quality Level	Method of Surveillance
Reporting	Reporting is timely, grammatically correct, accurate, and professional in appearance	98%	As Reported by Agency PM and recorded by the COR; Annual Program Review
Contract Management	Ensure all administrative actions are performed within the deadlines set forth by the PWS	100%	As Reported by Agency PM and recorded by the COR; Annual Program Review

System Tool Training	Ensure new users are trained within 30 days of providing access to the platform.	100%	As Reported by Agency PM and recorded by the COR; Annual Program Review
Platform Availability	Ensure that the platform is accessible to authorized users (e.g. system uptime availability) to support PWS requirements	>98%	As Reported by Agency PM and recorded by the COR; Annual Program Review

5. Period of Performance:
This BPA shall commence on the effective date of contract execution and shall continue in force for a base period of 5 years, with one 5 year option, for a total ordering period of 10 years. The total period of performance of any task award can not exceed ten (10) years.

In accordance with FAR 8.405-3(d)(3), Contractors may be awarded BPAs that extend beyond the current term of their GSA Schedule contract, so long as there are option periods in their GSA Schedule contract that, if exercised, will cover the BPA's period of performance.

Quoters will not be eligible for BPA award if their relevant GSA Schedule contract(s) will expire prior to the end of the BPA's awarded 10 year period of performance, if no further option periods on the relevant GSA Schedule contract(s) are available. The only exception to this rule is if a quoter has a continuous contract.

The use of a five-year base period and one, five-year option period under this BPA will reduce procurement lead time and associated costs for the option period; ensure continuity of BPA support; improve contractor performance; and facilitate longer-term contractual relationships with the BPA awardee.

Authorized Government Users: The Contractor shall make available/accessible to all authorized users of this BPA the database products and services listed above.

Technology Refreshment / Products and Services Improvement: The Contractor shall offer improvements to the database products and services offered under this BPA as capabilities become commercially available.

6. Key Personnel Requirements

All key personnel assigned to work under this requirement must meet the qualifications in Key Personnel requirements below. Experienced professional and/or technical personnel are essential for successful accomplishment of the work to be performed under this contract. The contractor agrees that such personnel shall not be removed or replaced from the contract work except as follows:

If one or more of the key personnel for whatever reason becomes or is expected to become unavailable for work under this contract for a continuous period exceeding 30 work-days, or is expected to devote substantially less effort to the work than indicated in the proposal, the contractor shall immediately notify the Contracting Officer and shall, subject to the concurrence of the Contracting Officer or their authorized representative, promptly replace such personnel with personnel of at least substantially equal ability and qualifications.

All requests for approval of substitutions or new hires hereunder must be submitted in writing at least 15 days (30 days if security clearance is to be obtained) in advance and provide detailed explanation of the circumstances necessitating the proposed substitutions or new hires to the Contracting Officer. The request must contain a complete resume, along with requisite contact information, for the proposed person(s) and any other information requested by the Contracting Officer to approve or disapprove the proposed substitution. The Contracting Officer or their authorized representative will evaluate such requests and promptly notify the contractor of his approval or disapproval thereof in writing. The contractor agrees that during the first 90 days of the contract performance period no key personnel substitutions will be permitted unless such substitutions are necessitated by an individual's sudden illness, death or termination of employment. In any of these events, the contractor shall promptly notify the Contracting Officer. All proposed substitutes must meet qualifications as delineated under Personnel Qualifications.

6.1. **Personnel Qualification Requirements:**

Program Manager

- Must possess a minimum of an advanced degree in a security or business intelligence field of study, **or** ten years of demonstrated management related work experience.
- Must have recent, within the last three years, hands-on experience in supply chain security intelligence analysis, technology capabilities supporting supply chain risk management and must be a recognized practitioner..

Technical Deployment Manager

- Must possess a minimum of an advanced degree in engineering, computer science or related scientific discipline, **or** 15 years of related scientific work experience;
- Must be uniquely skilled expert in data analytics or related fields supporting recent capability deployment activities, within the last three years.

7. IT Security Considerations

Contractors entering into an agreement for service to government activities will be subject to IT security standards, policies, reporting requirements, and governmentwide laws or regulations applicable to the protection of governmentwide information security,

Cybersecurity and SCRM are dynamic areas with developing regulations and requirements as evidenced by the ongoing development of the Cybersecurity Maturity Model Certification (CMMC) 2.0 framework by the Department of Defense (DoD), as well as National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, SP800-161, SP 800-171 and SP 800-172. As the SCRIPTS BPA will be a governmentwide acquisition vehicle, with potential customers of both civilian and defense organizations, it is important for the vehicle to remain relevant in light of changing requirements (see Attachment 4, Cybersecurity & Supply Chain Risk Management (SCRM) References).

The theft of intellectual property and Controlled Unclassified Information (CUI) through malicious cyber activity threatens not only the economic security of the United States, but our national security as well. Nation states, criminal and terrorist organizations, and rogue individuals will continue to target the defense industrial base as well as Government agencies and commercial entities in order to disrupt operations and/or undercut our technological advantages.

While CMMC is currently a DoD initiative, it may also have utility as a baseline for civilian acquisitions. SCRIPTS BPA quoters are encouraged to monitor, prepare for and participate in acquiring CMMC certification once CMMC 2.0 standards are promulgated.

Quoters should be aware of developing CMMC 2.0 and SCRM requirements by implementing the appropriate NIST SP 800-series documents, which are foundational to CMMC 2.0, FedRAMP, and other security programs. Once CMMC requirements have been finalized, GSA reserves the right to update the BPA with any applicable FAR clauses and provisions. Additional cybersecurity and SCRM requirements may be included on individual task orders by the issuing agency OCO. These requirements may vary on individual orders based on the security needs and criticality assessment of the ordering agency.

7.1 Cybersecurity Supply Chain Risk Management Plan
The quoter shall develop and operationally implement a Cybersecurity Supply Chain Risk Management (C-SCRM) plan that addresses system integrity through operational cyber hardening of their commercial infrastructure to ensure resilience against adversarial cyber-attacks within their ecosystem. The plan should be submitted to the government as part of their proposal submission and updated semi-annually, or as mutually agreed upon, to address progress and operational execution against the plan.

7.1.1 The SCRM plan, implementation, and risk assessment methodology processes shall follow Appendix D and E of NIST SP 800-161 Revision 1 (or current revision) (https://csrc.nist.gov/publications/detail/sp/800-161/final) and NISTIR 7622 (https://csrc.nist.gov/publications/detail/nistir/7622/final) guidelines.

7.1.2 Cybersecurity Supply Chain Risk Management (C-SCRM) Plan Submission
To ensure quoters remain aware of and are implementing emerging C-SCRM requirements over the life of the BPA, the SCRIPTS BPA C-SCRM Plan must be submitted to scrmtool@gsa.gov as indicated in PWS Section 9, Deliverables.

GSA will provide a C-SCRM Plan template to contractors prior to the submission dates indicated in PWS Section 9, Deliverables. This template must be utilized for preparation and submission of the required C-SCRM Plan. The C-SCRM Plan template may be updated by GSA throughout contract performance to reflect current SCRM factors and authoritative guidance. The C-SCRM Plan template may include, but will not limited to the following sections and will identify additional risk factor elements within Section 11 identified below:

1. Cover Page
2.Table of Contents
3. C-SCRM Plan Approval
4. System Name and Identifier
5. System Description
6. System Information Type and Categorization
7. System Operational Status
8. Role Identification
9. System/Network Diagrams, Inventory and Life Cycle Activities
10. Information Exchange and System Connections
11. Security Control Details (Minimum Control Baseline)
12. Contingencies and Emergencies
13. Revision and Maintenance
14. Acronym List
15. Terms and Definitions
16. References
17. Attachments
18. Related Laws, Regulations and Policies
19. C-SCRM Activities and Life Cycles

In the event GSA identifies necessary revisions to the submitted C-SCRM plan, a revised plan must be resubmitted within 30 days of notice from GSA. Failure to resolve any identified deficiencies in a timely manner may result in Government action, up to and including contract termination.

7.1.3 Risk Assessment
The Government may identify, assess, and monitor contractors' supply chain risks in connection with product and service offerings. The Government may use any information from public unclassified, classified, or any other sources for its analysis. Once complete, the Contractor agrees the Government may, at its own discretion, perform audits of supply chain risk processes or events. On-site assessments may be required. GSA may monitor the following supply chain risks:

1. Risk of Foreign ownership, control, or influence
2. Cyber threats
3. Other supply chain risks which could impact the company's vulnerability, such as financial performance issues

In the event supply chain risks are identified and corrective action becomes necessary, mutually agreeable corrective actions will be sought based upon specific identified risks. Failure to resolve any identified risk in a timely manner may result in Government action, up to and including contract termination.

7.2 Security: Facility Clearance Level (FCL)
If required by the Agency customer task order, the quoter must be capable of supporting customer task order requirements, up to and including Top-Secret/SCI. If defined by the ordering activity during the RFQ stage of the procurement, the quoter shall provide the necessary Facility Clearance Level (FCL) documentation (e.g. DD441 or agency equivalent) at the time of proposal submission and maintain it in accordance with National Industrial Security Program Operating Manual (NISPOM) to perform classified work throughout the duration of the effort. Verification of the FCL will be accomplished by GSA contacting the Defense CounterIntelligence and Security Agency (DCSA).

The government anticipates that the contractor could require access to classified information up to and including Secret/Top Secret/TS-SCI during the period of performance. If the prime contractor does not hold the appropriate FCL to support this activity, the government agency may sponsor the prime contractor's request for an FCL, which must be submitted within 60 (as appropriated based on when classified access is anticipated) calendar days of contract award. No classified access will be granted by the government until the FCL requirement has been satisfied. Based upon the lengthy process involved in obtaining an FCL, and the possibility of a negative outcome that would render the contractor unable to perform, the impact of not having an FCL could make the agency vulnerable to delays in performance. The SCRIPTS BPA program will not sponsor facility security clearances.

7.3 Security: Personnel Clearances
The quoter is responsible for providing personnel with appropriate security clearances to ensure compliance with Government security regulations, as specified in the ordering agency task order. The quoter must fully cooperate on all security checks and investigations by furnishing requested information to verify the quoter employee's trustworthiness and suitability for the position. Clearances may require Special Background Investigations (SBI), Sensitive Compartmented Information (SCI) access or Special Access Programs (SAP), or agency-specific access, such as a Q clearance or clearance for restricted data. Quoters should refer to task order solicitations for guidance on whether or not the customer agency will pay for the investigation or if the quoter is responsible for the cost of the investigation. The SCRIPTS BPA program will not sponsor personnel clearances.

8. Contract Administration
8.1. Place of Performance:

The primary place of performance will be at the contractor's work site. If required at the task order level, the customer may define alternate work locations as either onsite government customer location, or remote operating location.

8.2. Travel: N/A

8.3. Contracting Officer's Representative (COR):
An employee of the U.S. Government appointed by the contracting officer to administer the contract. Such appointment shall be in writing and shall state the scope of authority and limitations. This individual has authority to provide technical direction to the Contractor if that direction is within the scope of the contract, does not constitute a change, and has no funding implications. This individual does NOT have authority to change the terms and conditions of the contract. The Contracting Officer's Representative will be appointed at the time of BPA award.

Ordering Agencies will perform all COR responsibilities for any resulting task order(s). The ordering level agency will have a TPOC for any awarded task order(s). The COR responsibilities will be described in a COR Letter of Appointment provided by the ordering agency. The order level COR and TPOC will be responsible for quality assurance surveillance. Inspection and acceptance of all work performance, reports, and other deliverables under any will be performed by an individual appointed at the ordering level. The COR/TPOC at the agency level will be responsible for identifying where inspection and acceptance will occur.

8.4 Category Management Reporting:
During the PoP of this BPA it is projected that Transactional Data Reporting (TDR) will become a GSA MAS requirement. At that time, the Contractor must register in the government designated system in order to report transactional data in accordance with GSAR 552.216-75 deviation dated June 2022.

The contractor must provide the requested sales reporting data, outlined in Attachment 3, Category Management Reporting, electronically via the government designated system. The Contractor must adhere to the instruction and definitions for each reported data element as stated within the government designated system web page. The Government intends to post the reported hourly labor rates to the Prices Paid portal. The Prices Paid portal will be made available to Ordering Contracting Officers and agency program staff via a separate secured Government portal. Submitted data may be provided to BPA customers, upon request, to the extent permitted by Law. The reporting of sales reporting data is required for the following items, within the date specified in Section 9:

- Task Order Award
- Modification
- Invoices
- Zero Invoice (if applicable, when no invoice is shown for an active order month)

Data quality is significantly important; therefore, GSA may request from the Contractors corrections to the government designated system data, if applicable. Contractors must correct the government designated system data within the date specified below in Section 9, Deliverables.

8.5 Small Business Plan (Unrestricted Awards)
Quoters are to submit their most recent GSA Multiple Award Schedule contract electronic Subcontracting Reporting System (eSRS) signed report with their quote submission. Submission of this documentation should be labeled/saved as Company Name eSRS Report (i.e. "ABC Inc eSRS Report"). Reports are required for each large business CTA team member. Quoters will be rated more favorably if their most recent GSA Multiple Award Schedule contract Individual eSRS report reflects that they have met or exceeded their small business subcontracting goals percentage (**reference 2a. of the Quoters Multiple Award Schedule)** subcontracting report for individual contracts. For CTA teams, this means that each large business CTA team member must have met or exceeded their GSA Multiple Award Schedule contract small business subcontracting goals percentage in order to receive the favorable rating.

8.6 Integrated Quality Management System (IQMS)
The contractor should follow current International Organization for Standardization (ISO) 9001:2015 certification for services related requirements as part of their overall quality management program.

9. Deliverables
Deliverables shall be submitted to the COR designated within the contract. All deliverables shall be submitted using Microsoft Office suite of tools (for example, MS Word, MS Excel, MS PowerPoint), or Adobe PDF format, unless otherwise specified by the COR. Electronic submission shall be made via email, unless otherwise agreed to by the COR. The COR has the right to reject or require correction of any deficiencies found in the deliverables. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection and shall correct the deficiency within 5 days. The following table specifies the deliverables for this requirement:

Deliverables PWS Reference

ID	PWS Section	Title	Delivery	Frequency
1	Section 4	Non-Disclosure Agreement	Within 3 business days of award notification	Upon award and when a contract employee is backfilled
2	Section 4.15	SCRM Illumination Tool Training Report	10th day of every month.	Monthly

3	Section 4.31.6	Quarterly Program Status Report	Not later than the 10th day of every Third month.	Quarterly
4	Section 4.31.5	Annual Report	Within 30 days of anniversary of contract award	Annual
5	Section 7.1	Cyber SCRM Plan	Within 90 days after contract award	Semi-annually, as required per PWS
6	Section 8.4	Category Management Report	Not later than the 10th day of every Third month.	Quarterly, as part of Quarterly Program Status Report submission

10. Performance Requirement Summary Requirements

10.1 Performance Standards / Acceptable Quality Level

- All contractor personnel possess the skills needed to perform the required tasks as specified in the PWS.
- The Contractor's work products are suitable to support the full range of analysis as specified in the PWS.
- The contractor's personnel are qualified and adept at presenting clear, concise, factual reports free from political conclusions or any judgment of individual journalist(s). Editorial and typographical errors should be few.
- COR - review/government, personnel feedback Contractor Performance Assessment Reporting System (CPARS) evaluation/ratings

Reporting: Submit a quarterly program status report

The Program Status Report (PSR) accurately reflects progress, status, to include, but not be limited to, transactional data reporting; proactively identifies and addresses any problems or issues encountered; and recommended resolutions are feasible and likely to succeed in resolving issues.

Report is submitted by the 10th day of the third month following the previous quarters closing. Reports are grammatically correct and professional in appearance. Deviation with COR or designee approval. No more than 3 reports may be submitted by COB of the first Monday following the 10th day of the submission month; Draft documents contain minor typographical errors; Final documents are error free, COR Review Contractor Performance Assessment Reporting System (CPARS) evaluation/ratings

10.2 Hours of Work/Workload Management

The contractor ensures that sufficient staff will be available onsite at their facility, or at specified government work location(s), if required by the customer at the task order level, at all times

during core business hours to support assigned requirements. The contractor shall ensure its personnel accomplish the assigned tasks within agreed upon schedules, and at an acceptable level of quality. The Contractor ensures that sufficient staff is available during core business hours to proactively interact with clients and complete the requirements specified in the PWS. The contractor will also ensure the government assigned COR, whether designated at the task order level location or designated BPA level, is informed of developments with assigned actions. COR review/government personnel feedback Contractor Performance Assessment Reporting System (CPARS) evaluation/ratings. Additionally, if required, the contractor shall ensure personnel are available to accomplish outside of US operating hours in support of OCONUS regions.

10.3 Services and Deliverables

The Contractor provides the full range of services required to support the requirements addressed in section 4 of the PWS. The Contractor provides competent expertise and analysis that is consistent with the quality levels specified in the PWS. Deliverables are factual, well-written, 99% free of grammatical errors or misspellings, and free from political conclusions drawn by the analyst or any judgment of individual journalists. Writing meets college Baccalaureate degree standards for English grammar, spelling, and composition. Deliverables are accomplished by the due date/time specified in Section 9 of the PWS. Random review of work products by the CORz, as required, and feedback from appropriate Government sources. Contractor Performance Assessment Reporting System (CPARS) evaluation/ratings.

ATTACHMENT 1

Draft Risk Categorization Matrix (Small Business + Unrestricted)	
Risk Category	**Proposed Definitions**
FINANCIAL	The condition in which a supplier cannot generate revenue or income resulting in the inability to meet financial obligations. This is generally due to high fixed costs, illiquid assets, or revenues sensitive to economic downturns. Financial distress can lead to the inability to meet contractual obligations, hostile takeovers, or bankruptcy.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	A company is considered to be operating under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts and/or programs which support national security.
POLITICAL & REGULATORY	The weakness of the political powers and their legitimacy and control. Inadequacy of the control schemes, policies and planning, or broad political conditions. Includes terrorism, government policy changes, systematic corruption, and energy crises in the international marketplace. This can occur when changes in laws or regulations materially impact a security, business, sector or market. New laws and regulations enacted by the government or regulatory body can increase costs of operating a business, reduce the attractiveness of investment, or change the competitive landscape. Includes issues such as civil unrest or conflict and acts of terrorism that negatively impact supply chain operations. A certified act of terrorism must

	fall within the four identified descriptors determined by the Terrorism Risk Insurance Act (TRIA) and the Secretary of Treasury.
COMPLIANCE	Inability to comply with a wide-arching set of guidelines, policies, laws, and/or agreements established to avoid impact to national security.
TECHNOLOGY & CYBER SECURITY	Involves the management of cybersecurity requirements for information technology systems, software and networks, which are driven by threats such as cyber-terrorism, malware, data theft and the advanced persistent threat (APT). Technology risks include vulnerabilities and exposures of systems components and information systems produced by a specific supplier. Common risks include weaknesses in computation logic (code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity or availability.
Draft Additional Risk Categorization Matrix (Unrestricted Only)	
Risk Category	**Proposed Definitions**
MANUFACTURING & SUPPLY	Occurs when a supplier cannot fulfill the supply of a product to meet market demand. This can be due to reduced throughput or production delays caused by equipment down-time, capacity constraints, and delays in material delivery. Additional concerns include availability of supply, sole-source, and concentration within a singular country creating over-reliance.
TRANSPORTATION & DISTRIBUTION	Occurs when there is a dynamic disruption within the transportation and logistics of a product from one point to another. The transportation industry is among the most risk-prone of all industries, due to accidents, losses of cargo, driver shortages, and deteriorating infrastructure. These risks can

	cause shipment delays, supply chain disruptions, increased costs, and damaged reputations. In addition, the inability to predict and plan for disruptions in the logistics plan presents risk in meeting delivery requirements and maintaining operations.
PRODUCT QUALITY & DESIGN	Occurs due to inherent design and quality problems (e.g., raw materials, ingredients, production, logistics, and packaging) in which the part does not meet performance specifications and quality standards set by industry or DoD. Includes the detection of a part that was illegally created and sold under false pretenses. The part has not faced industry standard tests during the production phase (e.g., pressure testing) to ensure sustainability during usage. Counterfeit and non-MILSPEC parts pose significant risk to the function and safety of the system through malicious intrusion via backdoor exposures; increased maintenance costs due to depreciation in quality; and added stresses due to the parts inability to function at true capacity.

End of Attachment 1

ATTACHMENT 2

Draft Risk Categorization Matrix[4]		
Risk Category	**Risk Sub-Category**	**Proposed Sub-Category Definition**
FINANCIAL	Bankruptcy	The state of being completely lacking particular quality or value.
FINANCIAL	Financial Crimes	Financial crime refers to all crimes committed by an individual or a group of individuals that involve taking money or other property that belongs to someone else, to obtain a financial or professional gain.
FINANCIAL	Liquidity Risk	The risk of incurring losses resulting from the inability to meet payment obligations in a timely manner when they become due or from being unable to do so at a sustainment cost
FINANCIAL	Costs Overruns	A cost overrun, also known as a cost increase or budget overrun, involves unexpected, incurred costs. When these costs are in excess of budgeted amounts due to a value engineering underestimation of the actual cost during budgeting, they are known by these terms. Cost overruns are common in infrastructure, building, and technology projects and Weapon Systems.
FINANCIAL	Cyclical Risk	Cyclical risk is the risk of business cycles or other economic cycles adversely affecting the returns of an investment, an asset class or an individual company's profits.
FINANCIAL	Dependence on Defense Contracts	Consider DoD sales relative to total global sales for the facility. "Mixed" market is ~50% DoD; "Significant" is ~>60% for DoD or >60% for non-DoD; Very Strong or very weak

[4] OUSD (A&S) Policy Memo, *Supply Chain Risk Management Draft Taxonomy*, dated 10/28/2022

		DoD dominance can be risky for different reasons: High dependence on DoD contracts makes a facility more susceptible to DoD funding decisions. Low dependence on contracts makes the DoD more susceptible to business decisions by the facility.
FINANCIAL	Lack of Funding Sources	(1) Funding is money which a government or organization provides for a particular purpose. If sufficient funding is unavailable, it will limit the provider's ability to meet requirements. (2) An absence or limit in the assortment of capital a business can access to reinvest into business operations.
FINANCIAL	Offshore Leaks/ Database	The International Consortium of Investigative Journalists (ICIJ) Offshore Leaks Database represents a large set of relationships between people, companies, and organizations involved in the creation of offshore companies in tax-haven territories, mainly for hiding their assets.
FINANCIAL	Operational Efficiency Risk	In a business context, operational efficiency is a measurement of resource allocation and can be defined as the ratio between an output gained from the business and an input to run a business operation. When improving operational efficiency, the output to input ratio improves. Operational risk summarizes the uncertainties and hazards a company faces when it attempts to do its day-to-day business activities within a given field or industry. A type of business risk, it can result from breakdowns in internal

		procedures, people and systems-as opposed to problems incurred from external forces, such as political or economic events, or inherent to the entire market or market segment, known as systematic risk. Operational risk can also be classified as a variety of unsystematic risk, which is unique to a specific company or industry.
FINANCIAL	Profitability Measures	Profitability ratios are a class of financial metrics that are used to assess a business's ability to generate earnings relative to its revenue, operating costs, balance sheet assets, or shareholders' equity over time, using data from a specific point in time.
FINANCIAL	Solvency, Credit Risk	Solvency is the ability of a company to meet its long-term debts and financial obligations. Solvency can be an important measure of financial health, since it's one way of demonstrating a company's ability to manage its operations into the foreseeable future. The quickest way to assess a company's solvency is by checking its shareholders' equity on the balance sheet, which is the sum of a company's assets minus liabilities.
FINANCIAL	Unstable Payment Performance	When a company does not consistently "transfer money, goods or services in exchange for goods and services in acceptable proportions that have been previously agreed upon by all parties involved".
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Partnership with State-owned Entity	A state-owned enterprise (SOE) or government-owned enterprise (GOE) is a business enterprise where the government or state has significant control through full, majority, or significant minority ownership. Defining characteristics of SOEs are their distinct legal form and operation in commercial affairs and

		activities. While they may also have public policy objectives (e.g., a state railway company may aim to make transportation more accessible), SOEs should be differentiated from government agencies or state entities established to pursue purely nonfinancial objectives.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	State-owned Company	A state-owned enterprise (SOE) is a legal entity that is created by a government in order to partake in commercial activities on the government's behalf. A state-owned enterprise or government-owned enterprise is a business enterprise where the government or state has significant control through full, majority, or significant minority ownership.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Counterintelligence (Cl) Analysis	The process of examining and evaluating raw information to determine the nature, function, interrelationships, personalities, and intent regarding the intelligence capabilities of a foreign intelligence entity (FIE).
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Cl Collection	The systemic acquisition of intelligence information to answer Cl collection requirements.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Counterintelligence	Information gathered, and activities conducted to detect, identify, exploit and neutralize the intelligence capabilities and activities of terrorists, foreign powers and other entities directed against US national security.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Cyber Espionage	Cyber espionage is a form of cyber-attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity.
FOREIGN	Executive Poaching	The intentional action of one company to

OWNERSHIP CONTROL or INFLUENCE (FOCI)		hire an employee or group of employees currently employed at another company (many times a competing company).
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Foreign Intelligence Entity (FIE)	Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Industrial Espionage	Industrial espionage, economic espionage, corporate spying or corporate espionage is a form of espionage conducted for commercial purposes instead of purely national security. While economic espionage is conducted or orchestrated by governments and is international in scope, industrial or corporate espionage is more often national and occurs between companies or corporations.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Nationalization	A national government can transform privately owned businesses into state-owned businesses, which can enable foreign governments to enter existing supply chains.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Provenance	The extent to which a supplier relies on parts that are manufactured, sold, or distributed by companies that have part or whole foreign ownership or significant foreign influence.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Sabotage	1: destruction of an employer's property (such as tools or materials) or the hindering of manufacturing by discontented workers 2: destructive or obstructive action carried on by a civilian or enemy agent to hinder a

		nation's war effort 3a: an act or process tending to hamper or hurt 3b: deliberate subversion
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Theft of Trade Secrets	Trade secrets are a type of intellectual property that comprise formulas, practices, processes, designs, instruments, patterns, or compilations of information that have inherent economic value because they are not generally known or readily ascertainable by others, and which the owner takes reasonable measures to keep secret. In some jurisdictions, such secrets are referred to as confidential information.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Veiled Venture	An acquisition or economic-related action designed to camouflage nefarious intent of an individual, company, or country.
FOREIGN OWNERSHIP CONTROL or INFLUENCE (FOCI)	Weaponized Mergers and Acquisitions (M&A)	The use by national governments of the tools of regulation of M&A to advance, explicitly or implicitly, domestic political and trade agendas.
POLITICAL & REGULATORY	Terrorism	The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives
POLITICAL & REGULATORY	Watch List	The watch list is used by government agencies with a national security mission to support: Visa and passport screening (Department of State), International travel into the U.S. (U.S. Customs and Border Protection), and air passenger screening for terrorism (Transportation Security Administration).
POLITICAL & REGULATORY	Border Delays	Border delays can result in the timely delivery of materials/items.
POLITICAL &	Corruption	Corruption is dishonest behavior by those

REGULATORY		in positions of power, such as managers or government officials. Corruption can include giving or accepting bribes or inappropriate gifts, double-dealing, under-the-table transactions, manipulating elections, diverting funds, laundering money, and defrauding investors.
POLITICAL & REGULATORY	Environmental Protection Agency (EPA)	The mission of EPA is to protect human health and the environment.
POLITICAL & REGULATORY	Exposure (Potential Political)	The condition of being exposed to several events: such as: • the condition of being presented to view or made known • the condition of being unprotected especially from severe weather • the condition of being subject to some effect or influence • the condition of being at risk of financial loss
POLITICAL & REGULATORY	Government Collapse	State collapse, breakdown, or downfall is the complete failure of a mode of government within a sovereign state.
POLITICAL & REGULATORY	Government Policies	All DoD Policies/Regulations such as: DoD Acquisition process, DoD Acquisition and Supply regulations, Intel, Information Technology, Industrial Base, Domestic and Global transportation regulations
POLITICAL & REGULATORY	Interstate conflict (War or Armed Conflict)	Interstate conflict involves violence between two or more states
POLITICAL & REGULATORY	New Regulations, Changes in Policy (e.o., Trade Policy)	Changes in government policies or regulations that impact the supply chain.
POLITICAL & REGULATORY	Political/Government Changes	The risk that political changes or instability in a country could pose to a supply chain. Instability could stem from a change in

		government, legislative bodies, other foreign policymakers or military control. Political risk is also known as "geopolitical risk," and becomes more of a factor as the time horizon of investment gets longer. Government risk manifests when the actions of government increase uncertainty with respect to an organization, project or activity. An example of government risk is when poor behavior of an industry or sector leads to a government policy or regulatory response.
POLITICAL & REGULATORY	Territorial Disputes on trade routes	A trade route is a logistical network identified as a series of pathways and stoppages used for the commercial transport of cargo. Territorial disputes involve disagreement about who controls a particular territory or trade route.
POLITICAL & REGULATORY	Trade Wars	Trade war happens when one country retaliates against another by raising import tariffs or placing other restrictions on the other country's imports.
COMPLIANCE	Contractor Misconduct	When companies that sell goods or services to the government violate laws or regulations or are the subject of misconduct allegations in their dealings with the government, individuals, or private entities.

COMPLIANCE	Fraud (Procurement and Government)	Fraudulent activities by Federal or State employees, contractors, subcontractors, or any other participants on government contracts. Suspected fraudulent activities include, but are not limited to: · falsifying information on contract proposals · using Federal funds to purchase items that are not for Government use · billing more than one contract for the same work · billing for expenses not incurred as part of the contract · billing for work that was never performed, falsifying data · substituting approved materials with unauthorized products · misrepresenting a project's status to continue receiving Government funds · charging higher rates than those stated or negotiated for in the bid or contract · influencing government employees to award a grant or contract to a particular company, family member, or friend.
COMPLIANCE	Human Rights	Rights regarded as belonging fundamentally to all persons (e.g., freedom from unlawful imprisonment, torture, and execution).
COMPLIANCE	Legal and Reputational	Examples include lawsuits, discrimination, and other law enforcement actions.
COMPLIANCE	Past suspension or Debarment	Suspend - to temporarily pause or delay work with the option to continue later. This action must be taken by a suspending official and executed in accordance with FAR 9.4. Debar - to disqualify the person or company from receiving contracts. Must be completed by a debarring official and executed in compliance with FAR 9.4.

COMPLIANCE	Trafficking in Persons	"Trafficking in persons," "human trafficking," and "modern slavery" are umbrella terms – often used interchangeably – to refer to a crime whereby traffickers exploit and profit at the expense of adults or children by compelling them to perform labor or engage in commercial sex.
COMPLIANCE	Antitrust / Monopolistic Practices	Practices that unduly restrain competitive trade. Monopolistic practices - Companies' actions to create a monopoly. A monopoly refers to when a company and its product offerings dominate a sector or industry. Monopolies can be considered an extreme result of free-market capitalism in that, absent any restriction or restraints, a single company or group becomes large enough to own all or nearly all of the market (goods, supplies, commodities, infrastructure, and assets) for a particular type of product or service. The term monopoly is often used to describe an entity that has total or near-total control of a market.
COMPLIANCE	Conflict Minerals and Raw Materials in Supply Chain	Natural resources extracted in a conflict zone. In the United States, companies must report on their use and sourcing of tin, tantalum, tungsten and gold and raw materials.
COMPLIANCE	Contract Non-Compliance	Non-compliance occurs when one party in a contract does not fulfill his or her obligations.
COMPLIANCE	Import/Export Violation	Both the deliberate and non-deliberate violation of the customs laws of the United States.
COMPLIANCE	Defective Pricing	Result of CosUPricing Data (C/PD) that was certified by a contractor to be accurate, current, and complete but was

		not.
COMPLIANCE	Ethics Violation	A violation of moral principles that govern a person's behavior or the conductinQ of an activity.
COMPLIANCE	Forced Labor	Forced labor occurs when individuals are compelled to provide work or service through the use of force, fraud, or coercion.
COMPLIANCE	Insider Threat	Insider threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization.
COMPLIANCE	Occupational Workers Health and Safety (OSHA)	Safe and healthful working conditions for workers by setting and enforcing standards and by providing training, outreach, education and assistance.
COMPLIANCE	Securities and Exchange Commission (SEC) Enforcement Action	Actions that take place by the SEC to address misconduct that arose from or led to financial crimes.
TECHNOLOGY & CYBER SECURITY	Data Breach	A data breach is a security violation, in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.
TECHNOLOGY & CYBER SECURITY	Critical Hardware/Software Vulnerability	A weakness in automated system security procedures, administrative controls, internal controls, and so forth that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.
TECHNOLOGY & CYBER SECURITY	Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or destroying the integrity of the data or stealing controlled information.

TECHNOLOGY & CYBER SECURITY	Information Technology (IT) Disruption/Connectivity Issues	An IT issue that disrupts normal business operations such as an outage, errors while implementing new technology, ransomware, or IT overloads
TECHNOLOGY & CYBER SECURITY	IT Implementation Failure	A new system implementation or upgrade that fails to a degree where normal business operations are negatively impacted.
TECHNOLOGY & CYBER SECURITY	IT Obsolescence	When a technical product or service is no longer needed or wanted even though it could still be in working order. Technological obsolescence generally occurs when a new product has been created to replace an older version.
TECHNOLOGY & CYBER SECURITY	Loss or Theft Of DCI/PII [Discharge of Classified Information (DCI); Personally Identifiable Information (PII)	PII--The removal or unlawful taking of information that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may include a combination of gender, race, birth date,geographic indicator, and other descriptors. CII--The removal or unlawful taking of information that a defense organization has determined to be valuable to an adversary. This information may vary based on the organization's role.
TECHNOLOGY & CYBER SECURITY	Malicious Intrusion	Intrusions that take place anytime a bad actor gains access to an application with the intent of causing harm to or steal data from the network or user
TECHNOLOGY & CYBER SECURITY	OPSEC / INFOSEC Violation	OPSEC (operational security) is an analytical process that classifies information assets and determines the

		controls required to protect these assets. After vulnerabilities have been determined, the next step is to determine the threat level associated with each of them. OPSEC encourages managers to view operations or projects from the outside in, or from the perspective of competitors (or enemies) in order to identify weaknesses. If an organization can easily extract their own information while acting as an outsider, odds are adversaries outside the organization can as well. Completing regular risk assessments and OPSEC is key to identifying vulnerabilities.
TECHNOLOGY & CYBER SECURITY	Unsecure Networks or Systems	An unsecured network or system lacks intrusion detection and prevention capability.
MANUFACTURING & SUPPLY	Outsourcing	Outsourcing is the business practice of hiring a party outside a company to perform services and create goods that traditionally were performed in-house by the company's own employees and staff.
MANUFACTURING & SUPPLY	Reseller/3rd Party Vendor/Middleman	A person or company that sells something they have bought from someone else.
MANUFACTURING & SUPPLY	Sole Source Dependency	Only one supplier for the required item is available.
MANUFACTURING & SUPPLY	Adjacency Risk	When separate industries (e.g. auto industry and defense sector) compete for limited resources (e.g., microchips).
MANUFACTURING & SUPPLY	Agriculture	Agriculture is the art and science of cultivating the soil, growing crops and raising livestock. It includes the preparation of plant and animal products for people to use and their distribution to markets. Agriculture provides most of the world's food and fabrics.

MANUFACTURING & SUPPLY	Concentration Risk	The probability of loss likely to arise due to over-dependence on a single vendor, concentration risk is further exacerbated when such a vendor specializes in a specific industry.
MANUFACTURING & SUPPLY	Equipment Down Time	Equipment downtime refers to the amount of time that equipment is not operating, whether that is a result of unplanned equipment failure (e.g., a fault or broken part) or planned downtime (e.g., necessary downtime for preventive maintenance).
MANUFACTURING & SUPPLY	Extended Lead Times	Unplanned and/or unexpected time it takes between order initiation and product delivery.
MANUFACTURING & SUPPLY	Industrial Capability	Industrial capability is "the ability of industry to accomplish (make, create, destroy, etc.) a result (product, information, objective, etc.)." This drives both the larger products (e.g., can we make airplanes?) and more specifics (e.g., can we make a stealth covering for legacy airplanes to avoid aerial reconnaissance while on the tarmac?)
MANUFACTURING & SUPPLY	Industrial Capacity	Industrial capacity is "the amount (e.g., quantity) of industrial capability" or "the amount (e.g., quantity) of the ability of industry to accomplish a result". This could include products (e.g., industry can make one item per month with existing lines), services (e.g., industry can service one plane per hour), and changes (e.g., if industry received $XX this month they could increase by YY production lines next month to make 50 items per month).
MANUFACTURING & SUPPLY	Inventory or Capacity Incidents	Loss of inventory or capacity from events. This may be a loss from building failure, access restrictions, etc
MANUFACTURING	Inventory	A stockout, or out-of-stock (OOS) event is

& SUPPLY	Stockout/Material Shortages	an event that causes inventory to be exhausted.
MANUFACTURING & SUPPLY	Material Sources	The origin of materials which have been used to form or manufacture a product generally represented as the N-1 Supply Tier. This includes direct material used in the product and indirect material used in production and manufacturing, e.g., castings.
MANUFACTURING & SUPPLY	Obsolescence/ Diminishing Manufacturing Sources and Material Shortages (DMSMS)	Obsolescence is defined as the loss or impending loss of original manufacturers of items or suppliers of items or raw materials. This type of obsolescence is commonly referred to as DMSMS (Diminishing Manufacturing Sources and Material Shortages) within the Department of Defense, which is caused by the unavailability of technologies or parts that are necessary to manufacture or sustain a system. Due to the length of the system's manufacturing and support life, and unforeseen life extensions to the support of the system longer than its planned end of support date, the parts and other resources necessary to support the system become unavailable before the system's demand for the parts or other resources ends.
MANUFACTURING & SUPPLY	Order Fulfillment	The complete process from point of sales inquiry to delivery of a product to the customer.
MANUFACTURING & SUPPLY	Parts/Spares Inventory Shortages	Inadequate supplies of spare parts on hand for maintenance and repairs.
MANUFACTURING & SUPPLY	Reclamation/Utilization	Process to reclaim whole or essential components and materials for manufacturing either the same or alternate products. Reutilization is using components and materials for the same, similar, or differing purpose (e.g., using ships again in different missions or sinking to build reefs)

MANUFACTURING & SUPPLY	Single Source	A particular supplier is purposefully chosen by the buying organization, even when other suppliers are available
MANUFACTURING & SUPPLY	Throughput/Production Delays	A delay in the amount of a product or service that a company can produce and deliver to a client within a specified period of time.
MANUFACTURING & SUPPLY	Underdeveloped Product Pipeline	Used to transmit fuel and natural gas or derivatives to manufacturing and supply facilities. The extent to which the Original Equipment Manufacturer (OEM) is resilient to delays in supply chain capacity and development needed to meet extant and nascent manufacturing requirements
TRANSPORTATION & DISTRIBUTION	Poor Delivery Performance	Poor delivery performance includes incorrect and incomplete shipments, shipments to the wrong location, and late shipments.
TRANSPORTATION & DISTRIBUTION	Accidents	An incident that happens unexpectedly and unintentionally, typically resulting in damage, injury, and negatively impacts the transportation network.
TRANSPORTATION & DISTRIBUTION	Changes in Trade Policy (Containers in Ports)	See Office of the U.S. Trade Representative (https://ustr.gov/)
TRANSPORTATION & DISTRIBUTION	Loss of Cargo	Cargo loss means any loss or destruction that occurs while the cargo is moved within distribution channels.
TRANSPORTATION & DISTRIBUTION	Poor Shipment and Delivery Accuracy	Shipment accuracy implies that items are properly fulfilled, packed, and delivered in accordance with the customer's requirements.
TRANSPORTATION & DISTRIBUTION	Transportation Network Disruption	Disruptions to the transportation network can cause delays or missed shipments of material and items.
PRODUCT QUALITY &	Counterfeit Parts	The unlawful or unauthorized reproduction, substitution, or alteration that

DESIGN		has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified item from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used items represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.
PRODUCT QUALITY & DESIGN	Non-Conforming Parts	Non-conforming materials are any product or parts that are defective, counterfeit or do not meet the requirements.
PRODUCT QUALITY & DESIGN	Non-MILSPEC (Military Specification) Parts	Non-MILSPEC parts items may not conform to military specifications and could result in product failure.
PRODUCT QUALITY & DESIGN	Product Characteristics	Product characteristics can inform decisions on whether products can be interchangeable or substitutable.
PRODUCT QUALITY & DESIGN	System/Parts Performance Failure	Performance is a measurement of either work or time, for example, system-related work accomplished within a given time and the time required to complete a task or iob, based upon past performance.
PRODUCT QUALITY & DESIGN	Unreported Supplier Recalls	Unsupported Product Recall means recalls unsubstantiated by documentation or receipts incurred by third parties selling a Product(s) that is included in a Recall(s) to the end user(s).

End of Attachment 2

ATTACHMENT 3
Category Management Reporting

The Contractor must submit a Category Management Report (CMR) for all orders issued, modifications, invoices within the date specified in the Performance Work Statement (PWS), Section 9, Deliverables. If applicable, orders issued by the GSA Assisted Acquisition Service from the BPA, via the AAS Business System Portal (ASSIST), will be populated into the government designated system. Refer to the government designated system instructions for the reporting process. The data elements identified below are representative of what is required in the government designated system (e.g. Sales Reporting Portal (SRP)). It is mandatory to complete the data elements in the format outlined in the government designated system instructions.

a. Contract/BPA Number
b. Order Number/PIID
c. Order Description of Deliverable
d. Primary NAICS
e. Special Item Number (SIN) Number
f. Manufacturer/Developer Name
g. Manufacturer/Developer Product Number
h. Universal Product Code
i. Unit of Measure
j. Quantity of Item Sold
k. Prices Paid per Unit (USD$)
l. BPA Unit Price (USD$)
m. Total Price (USD$)
n. Non-Federal Entity (YES/NO)
o. GSA Assisted Services (YES/NO)
p. RFQ Submitted Date
q. Award Date
r. Period of Performance (Start)
s. Period of Performance (End)
t. Initial Obligated/Funded Amount
u. Total Obligated/Funded Amount
v. Ordering Agency/Bureau
w. Ordering Agency/SubTier
x. Issued By DODAAC/AAC
y. Ordering Contracting Officer Name
z. Issued By Email
aa. Place of Performance

bb. Attachments (Award Documents/SOW/SOO/PWS)
cc. Modification Number, if applicable
dd. Modification - Award Date
ee. Modification - Period of Performance
ff. Modification - Type
gg. Modification - Order Description
hh. Modification - Obligated/Funded Amount
ii. Invoice - Reporting Period
jj. Invoice -Number
kk. Invoice - Paid Date
ll. Invoice - Amount
mm. Invoice - Contract Line Item Number
nn. Invoice - Line Item Identifier
oo. Invoice - Line Item Type
pp. Zero Invoice (if applicable)
qq. Services - Employee Security Clearance Level (if applicable)
rr. Services - Employee Labor Category
ss. Services - Employee Applicable Labor Law (SCA, DBA, Exempt, or N/A)
tt. Services - Employee Location (Zip Code)
uu. Services - Employee Indirect Hourly Costs (if applicable)
vv. Services - Type of Work Performed
ww. Services - Place of Performance (Government Site, Contractor Site, Remote, or N/A)

CONTRACT LINE ITEM NUMBER (CLIN) STRUCTURE

The Contractor must apply one or more of the following Program CLINs when reporting invoices in the government designated system.

BPA REPORTING CLIN	REPORTING LINE TYPE
See Attachment X	SCRIPTS Labor Categories
L00	Labor Hour Rate & Labors Hours
F00	Zero Invoice
H00	Fixed Price Services
A00	Order Level Materials (OLM)

SALES REPORTING DATA FIELD DEFINITIONS

a. Contract/BPA Number - GSA contract number - (ex: 47QTCAXXDXXXXXX)
b. Order Number/PIID - the award document number. Order Number assigned on Award Document and reported to FPDS-NG. For example, on a SF26 -"CONTRACT (Proc. Inst. Indent.) NO." Block 2; SF33 - "CONTRACT NO." Block 2; SF1449 "CONTRACT NO." Block 2; GSA300 -"ORDER NO." Block 2. It may also be known as the Procurement Instrument Identifier (PIID). Different for every order.
c. Order Description - Descriptive language that provides a short summary of the activities or objectives of the task order.
d. Primary NAICS - this is the NAICS code that should be identified on the award document or other procurement documentation that reflects the primary nature of the work planned on the task order.
e. Special Item Number (SIN) - GSA designated special item number which the service or technical support is being provided under the vendor's catalog.
f. Manufacturer/Developer Name - self explanatory.
g. Manufacturer/Developer Product Number - SKU or alphanumeric identifier assigned to product in reference vendor catalog, if applicable.
h. Universal Product Code - vendor's unique code identifier for Services, if applicable.
i. Unit of Measure - is the defined magnitude of the quantity that is used as standard measurement of defined service. (e.g. Unit, Seat, Subscription, Report, Labor Hour)
j. Quantity of Item Sold - this field defines how many items were sold; or hours in the case of services.
k. Prices Paid per Unit (USD$) - the net sale price for each line item; the reported price paid per unit must be fully burdened hourly rate for services.
l. BPA Unit Price (USD$) - the discounted BPA ceiling price for each line item
m. and Total Price (USD$) - This is a system calculated field, it is the product of quantity price paid. The formula used to calculate is "Total Price"=ROUND((Quantity of Item Sold *Unit price).
n. Non-Federal Entity (YES/NO) - This describes whether the customer making the order is a Federal Government Entity or other authorized user such as cost reimbursement contract per FAR 51, state/local or Non-Government Organization.
o. GSA Assisted Services (YES/NO) - indicator to reflect whether or not the task order was awarded by GSA Assisted Services or instead awarded as a direct procurement from another government agency.
p. RFQ Submitted Date - date that the Contracting Officer submitted the online Request for Quotation (RFQ) in the GSA eBUY portal
q. Award Date - this is the date that the Contracting Officer signs the award. If there is no signature date, then use the Effective date.
r. Period of Performance (Start) - date subscription/license or task award support begins.
s. Period of Performance (End) - date subscription/license or task award support ends.

t. Initial Obligated/Funded Amount - the total amount obligated on the initial award document. This value should not include any un-exercised options
u. Total Obligated/Funded Amount - the total amount obligated on the initial award document plus any additional increases or decreases on awarded order modifications. This value should not include any unexercised options. May also be called "Mod Oblig/Fund Amt".
v. Ordering Agency/Bureau - the name of the agency and bureau that is ordering the goods/services awarded on the task order.
w. Ordering Agency/SubTier - additional subtier organizational Ordering Agency information, if applicable (e.g. Operational or Unit Level below Agency level)
x. Issued By DODAAC/AAC - registered DoDAAC of issuing organization.
y. Issued By / Ordering Contracting Officer Name - self explanatory.
z. Issued By Email - contact email for Ordering Contracting Officer.
aa. Place of Performance - the city, state, zip code of the primary place of performance for the task order.
bb. Attachments (Award Documents/SOW/SOO/PWS) - attach copies of award documents, statements of work, performance work statements, etc. for the reported task order.
cc. Modification Number, if applicable - the value from the order mod award document.
dd. Modification - Award Date - the date that the contracting officer signs the order modification award document.
ee. Modification - Period of Performance - as defined in 2 C.F.R 200.77 is the time during which the non-Federal entity may incur new obligations to carry out the work authorized under the Federal award.
ff. Modification - Type - code representing the best description of the modification type.
gg. Modification - Order Description - a brief description of the nature of the task/delivery order mod. If Mod Type = Additional Work (other), Change Order, Administrative, or Other, then required. Otherwise, this field is optional.
hh. Modification - Obligated/Funded Amount - the increase or decrease dollar amount funded on the modification award, not including un-exercised options.
ii. Invoice - Reporting Period - month and year of report submission
jj. Invoice - Number - number on invoice paid by customer
kk. Invoice - Paid Date - date the invoice was paid by the customer.
ll. Invoice - Amount - current total amount invoiced against the task order
mm. Invoice - Contract Line Item Number - self explanatory. See table above.
nn. Invoice - Line Item Identifier - number assigned to the invoice line item. System generated field
oo. Invoice - Line Item Type - either the CLIN Description or the CLIN Code associated with the contract vehicle. System generated field (such as labor, travel, OLM, or some other type of invoice line item)
pp. Zero Invoice (if applicable) - the contractor has not invoiced with a customer for the reporting period on an awarded task order.
qq. Services - Employee Security Clearance Level (if applicable) - Security clearance held by contractor FTE performing the work (S, TS, TS/SCI, or TS/SCI/poly)

rr. Services - Employee Labor Category - is the primary labor category of the work performed as specified in the BPA award document.
ss. Services - Employee Applicable Labor Law (Services Contract Act, Davis-Bacon Act, Exempt, or N/A) - Applicable labor law for contractor FTE performing the work.
tt. Services - Employee Location (Zip Code) - where the contractor FTE performs his/her/their work (5-digit #).
uu. Services - Employee Indirect Hourly Costs (if applicable) - Hourly breakdown of indirect costs captured in the fully burdened hourly labor rate.
vv. Services - Type of Work Performed - high-level type of work that will be performed on a task order.
ww. Services - Place of Performance (Government Site, Contractor Site, Remote, or N/A) - indicates the type of site where work was performed

(End of Attachment 3)

Attachment 4

Cybersecurity & Supply Chain Risk Management (SCRM) References

Security is rapidly emerging as the "fourth pillar" of acquisition in addition to price, performance and delivery. Contractors will be required to comply with existing cybersecurity and SCRM requirements as well as implement new requirements that are established during the period of performance. Furthermore, Contractors should be aware that their cybersecurity and SCRM capabilities may impact their competitiveness as agencies increasingly incorporate cybersecurity and SCRM related requirements, evaluation factors and reporting at the task order level. Contractors entering into an agreement to provide service to Government activities are subject to information technology security (a/k/a cybersecurity) and SCRM laws, regulations, standards, policies and reporting requirements. Additional and/or tailored cybersecurity and SCRM requirements may be included in individual task orders by the issuing agency OCO. The Contractor must ensure that all applicable Commercial-Off-The-Shelf (COTS) and enabled products comply with ordering agency cybersecurity and SCRM requirements.

A. Laws

1. The Privacy Act of 1974, P.L. 93-579
2. The Clinger-Cohen Act of 1996, Pub. L. 104-106, Division E
3. The Federal Information Security Modernization Act of 2014, Pub. L. 113-283
4. Federal Information Technology Acquisition Reform Act (FITARA), Pub. L.113-291
5. Section 818 of the FY 2012 National Defense Authorization Act
6. Section 1634 of the FY 2018 National Defense Authorization Act

7. Section 881 of the FY 2019 National Defense Authorization Act
8. Section 889 of the FY 2019 National Defense Authorization Act (implemented by FAR 52.204-24 and FAR 52.204-25)
9. Sections 1631-1657 of the FY 2019 National Defense Authorization Act
10. Section 4713 of the SECURE Technology Act, Pub. L.115-390
11. The Federal Acquisition Supply Chain Security Act (FASCA) of 2020, Pub. L. 115-390
12. Secure 5G and Beyond Act of 2020, Pub. L.116-129

B. Executive Orders and Presidential Directives

1. Executive Order 13636, Improving Critical Infrastructure Cybersecurity
2. Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing
3. Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
4. Executive Order 13833, Enhancing Effectiveness of Agency Chief Information Officers
5. Executive Order 13859, Maintaining American Leadership in Artificial Intelligence
6. Executive Order 13870, America's Cybersecurity Workforce
7. Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain
8. Executive Order 14028, Improving the Nation's Cybersecurity
9. Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors

C. Policies of the Committee on National Security Systems

1. The policies presented under this topic address national security systems issues from a broad perspective. They establish national-level goals and objectives, all of which are binding upon all U.S. Government departments and agencies. http://www.cnss.gov/CNSS/issuances/Policies.cfm

D. OMB Circulars and Memoranda

1. Circulars (https://www.whitehouse.gov/omb/information-for-agencies/circulars/)
   a. A-130, Managing Information as a Strategic Resource
   b. A-123, Management's Responsibility for Internal Control
   c. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act
   d. A-11, Preparation, Submission and Execution of the Budget

2. Memoranda (https://www.whitehouse.gov/omb/information-for-agencies/memoranda/)
   a. M-19-18, Federal Data Strategy – A Framework for Consistency
   b. M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management
   c. M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program
   d. M-19-01, Request for Agency Feedback on the Federal Data Strategy
   e. M-18-23, Shifting From Low-Value to High-Value Work
   f. M-18-12, Implementation of the Modernizing Government Technology Act
   g. M-17-25, Reporting Guidance for Executive Order on Strengthening the

Cybersecurity of Federal Networks and Critical Infrastructure
h. M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government
i. M-15-14, Management and Oversight of Federal Information Technology
j. M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response
k. M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
l. M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents

E. National Institute of Standards and Technology (NIST)

1. Federal Information Processing Standards (FIPS)
   a. https://www.nist.gov/itl/fips-general-information
   b. https://www.nist.gov/standardsgov/compliance-faqs-federal-informationprocessing-standards-fips
2. Special Publication 800-series and 1800-series
   a. https://www.nist.gov/itl/nist-special-publication-800-series-general-information
   b. https://csrc.nist.gov/publications/sp800
   c. https://www.nist.gov/itl/nist-special-publication-1800-series-general-information
   d. https://csrc.nist.gov/publications/sp1800
3. Framework for Improving Critical Infrastructure Cybersecurity
   a. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
4. NICE Cybersecurity Workforce Framework Resource Center
   a. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurityworkforce-framework-resource-center

F. Cybersecurity and Infrastructure Security Agency

1. Information and Communications Technology Supply Chain Risk Management

G. Cybersecurity Maturity Model Certification

1. Cybersecurity Maturity Model Certification (CMMC 2.0)
2. CMMC Accreditation Body

H. Cloud Computing

1. NIST SP 500-291 (2011), NIST cloud computing standards roadmap
2. NIST SP 500-293 (2014), U.S. government cloud computing technology roadmap
3. NIST SP 800-144 (2011), Guidelines on security and privacy in public cloud computing
4. NIST SP 800-145 (2011), The NIST definition of cloud computing
5. ISO/IEC 17789:2014, Information technology -- Cloud computing -- Reference architecture
6. ISO/IEC 17826:2016, Information technology -- Cloud data management interface
7. ISO/IEC 18384-1:2016, Information technology — Reference Architecture for Service Oriented Architecture (SOA RA) — Part 1: Terminology and concepts for SOA
8. ISO/IEC 18384-2:2016, Information technology — Reference Architecture for Service Oriented Architecture (SOA RA) — Part 2: Reference Architecture for SOA Solutions

9. ISO/IEC 18384-3:2016, Information technology — Reference Architecture for Service Oriented Architecture (SOA RA) — Part 3: Service Oriented Architecture ontology
10. ISO/IEC 19086-1:2016, Information technology -- Cloud computing -- Service level agreement (SLA) framework
11. ISO/IEC 19086-2:2018, Cloud computing — Service level agreement (SLA) framework
12. ISO/IEC 19086-3:2017, Information technology — Cloud computing — Service level agreement (SLA) framework — Part 3: Core conformance requirements
13. ISO/IEC 19086-4:2019, Cloud computing — Service level agreement (SLA) framework
14. ISO/IEC 19941:2017, Information technology -- Cloud computing -- Interoperability and portability
15. ISO/IEC 19944-1:2020, Cloud computing and distributed platforms -- Data flow, data categories and data use — Part 1: Fundamentals
16. ISO/IEC DIS 19944-2, Cloud computing and distributed platforms — Data flow, data categories and data use — Part 2: Guidance on application and extensibility
17. ISO/IEC 20933:2019, Information technology — Distributed application platforms and services (DAPS) — Framework for distributed real-time access systems
18. ISO/IEC 22123-1:2021, Information technology — Cloud computing — Part 1: Vocabulary
19. ISO/IEC CD 22123-2.4, Information technology — Cloud computing — Part 2: Concepts
20. ISO/IEC 22624:2020, Information technology — Cloud computing — Taxonomy based data handling for cloud services
21. ISO/IEC TR 22678:2019, Information technology — Cloud computing — Guidance for policy development
22. ISO/IEC TS 23167:2020, Information technology — Cloud computing — Common technologies and techniques
23. ISO/IEC TR 23186:2018, Information technology — Cloud computing — Framework of trust for processing of multi-sourced data
24. ISO/IEC TR 23187:2020, Information technology — Cloud computing — Interacting with cloud service partners (CSNs)
25. ISO/IEC TR 23188:2020, Information technology — Cloud computing — Edge computing landscape
26. ISO/IEC TR 23613:2020, Information technology — Cloud computing — Cloud service metering elements and billing modes
27. ISO/IEC TR 23951:2020, Information technology — Cloud computing — Guidance for using the cloud SLA metric model
28. ISO/IEC TR 30102:2012, Information technology — Distributed Application Platforms and Services (DAPS) — General technical principles of Service Oriented Architecture
29. ISO/IEC 27017:2015, Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services
30. ISO/IEC 27018:2019, Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

I. Zero Trust

1. NIST framework for Improving Critical Infrastructure Cybersecurity, Version 1.1

2. NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments
3. NIST SP 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach For Security and Privacy
4. NIST SP 800-40 Revision 3, Guide to Enterprise Patch Management Technologies
5. NIST SP 800-46 Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
6. NIST SP 800-53 Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations
7. NIST SP 800-57 Part 1 Revision 4, Recommendation for Key Management: Part 1: General
8. NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide
9. NIST SP 800-63 Revision 3, Digital Identity Guidelines
10. NIST SP 800-92, Guide to Computer Security Log Management
12. NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
14. NIST SP 800-160 Vol. 2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach
15. NIST SP 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations
16. NIST SP 800-175B, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
17. NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
18. NIST SP 800-205, Attribute Considerations for Access Control Systems
19. NIST SP 800-207, Zero Trust Architecture
20. NIST SP 1800-3, Attribute Based Access Control
21. ISO/IEC 20243-1:2018, Information technology — Open Trusted Technology ProviderTM Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 1: Requirements and recommendations
22. ISO/IEC 20243-2:2018, Information technology — Open Trusted Technology ProviderTM Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 2: Assessment procedures for the O-TTPS and ISO/IEC 20243-1:2018
23. ISO/IEC 27001, Information Technology–Security Techniques–Information Security Management Systems
24. Federal Information Processing Standards 140-3, Security Requirements for Cryptographic Modules

(End of Attachment 4)