Task Order Performance Work Statement

Research related to Internet of Things (IoTs) Architecture and Cybersecurity Risk Management Framework
Task Order 7 under CRDI IDIQ

1. BACKGROUND
The Internet of Things (IoT) solutions are widely adopted and deployed across different industry sectors to solve specific business challenges to provide greater functional capabilities and produce telemetry data to provide analytics to increase productivity, reduce operation cost, improve quality of life, provide visibility, and make predictive decisions. IoT are becoming ubiquitous and enable the vertical markets to innovate at Internet scale and speed. These sensors are capable of generating large amounts of data, connecting directly to the Internet to transmit them and receive commands from large back-end data collections, analytics, and control systems in near real time. These added capabilities introduce a large attack surface that can minimize by adopting a risk management approach to reduce the impact to the system integrity, confidentiality, and availability. NIST's Computer Security Division (CSD) has conducted research in similar fields such as cyber physical systems and in particular smart grid and industrial control systems by publishing guidance to federal departments and agencies and industry sectors as well as documents on management strategies. More research is needed in the area, specifically identifying existing recommended practices and gaps in standards and technology.

2. SCOPE
The Contractor shall conduct research on IoT architectures, cybersecurity threats and recommended practices, and then analyze that research to develop countermeasures expressed in the NIST Cybersecurity Framework (CSF) and NIST SP 800-53 taxonomy that are mapped back to the sector specific regulations. The Contractor shall work with NIST to develop a NIST Interagency Report (NISTIR).

THIS IS A HYBRID LABOR HOUR AND FIRM FIXED PRICE TASK ORDER.

3. OBJECTIVES
The CSD objective for this tasking is to research and document a survey of the different IoT verticals or industry sectors such as Smart Cities, Connected Healthcare, Smart Buildings, Smart Homes, Transportation and Logistics, Industrial and Manufacturing, Smart Oil & Gas, Smart Agriculture, and Wearables. A taxonomy shall be developed for describing and classifying IoT systems based on the properties and characteristics of the components and their functionalities according to the usage model. For each of the selected verticals, a high level overlay of IoT functionality shall be developed to depict the industry sector specific reference model. Relevant security considerations driven by the current threat landscape and the relevant cybersecurity standards, guidelines, regulations, recommended practices, industry groups and consortiums applicable to IoT shall be researched and developed. The NIST Cybersecurity Framework structure shall be used to document the recommendations in the form of the NIST SP 800-53 security controls in the context of IoT using a data centric system threat modeling process as described in the draft NIST SP 800-154 (http://csrc.nist.gov/publications/drafts/800-154/sp800_154_draft.pdf). The ultimate output shall be a NISTIR, which shall be developed in collaboration with the NIST team and its content and findings will be driven by the research. The

publication shall target the U.S. Government departments and agencies of all sizes and types, keeping in mind that the findings may also be used by various industry sectors.

4. TASKS

4.1. CYBERSECURITY CONSIDERATIONS FOR INTERNET OF THINGS (IOT) – (LABOR HOUR)

4.1.1. Survey of the Different IoT Industry Sectors/Verticals

The contractor shall research and document a survey of the different IoT systems pertinent to various sectors such as Smart Cities, Connected Healthcare, Smart Buildings, Smart Homes, Transportation and Logistics, Industrial and Manufacturing, Smart Oil & Gas, Smart Agriculture, and Wearable. The sources shall originate from Industry groups, business trade organizations, Internet resources, and IT research and advisory groups. The deliverable shall include a document with a set of references describing the current landscape including adoption rate of the technology of IoT and the technologies used in each sector detailing their associated features and capabilities. The output shall include an internal draft and a final document with associated original resources.

4.1.2. Taxonomy for Describing and Classifying IoT

Based on the usage scenario per industry sector and class of technology, the contractor shall develop a taxonomy for describing and classifying IoT systems based on components and functionality. The contractor shall provide a vocabulary for describing the fundamental characteristics for IoT, their principles, their capabilities, relationship and dependencies to other IT components such as network and data analytics backend systems, their interfaces, their processing, storage, and communication capabilities, etc. The deliverable shall be a document capturing the definition, vocabulary, a classification model based on features, capabilities, etc. and a functional architecture of the IoT describing their interactions with other systems. The output shall include an internal draft and a final document.

4.1.3. Overlay of IoT Functionality

For each specific usage scenario, the contractor shall produce a high level overlay of IoT functionality depicted on top of the sector specific reference model. The contractor shall research and iterate the reference model for each vertical working with the NIST team. The contractor shall identify the architecture and functionality of each sector and overlay the sector specific architecture with a generalized architecture to determine which portions of the vertical are truly IoT centric. The deliverable shall be a document describing the sector specific reference model, the IoT architecture, the overlay and all associated information describing the mapping model. The output shall include an internal draft and a final document.

4.1.4. IoT Cybersecurity Threats, Standards, Guidelines, Recommended Practices, and Regulations

The contractor shall research and document relevant security and privacy considerations driven by the current threat landscape and apply a data-centric system threat modeling methodology. The contractor shall identify the relevant cybersecurity standards, guidelines, recommended practices, and regulations applicable to IoT. The deliverable shall be a document that maps IoT architecture, components and functionalities to include specific capabilities and the security and privacy requirements that should be considered based on the understanding of the current threat landscape that drives the threat modeling exercise and countermeasures as prescribed by various national and international Standards Development Organizations (SDOs), government, and industry groups or consortiums. The output shall include an internal draft and a final document with tables represented as an Excel spreadsheet to include all the relevant data.

4.1.5. Mapping of the findings to the NIST Cybersecurity Framework and associated SP 800-53 security controls

The contractor shall use the NIST Cybersecurity Framework (CSF) structure (most recent version) to document the security controls expressed in the NIST SP 800-53 Rev 4 to document the security controls applicable to IoT. The contractor shall use the proposed countermeasures developed in the previous task (4.1.4) to produce a security baseline targeted for each IoT class or technology grouping and sector. The output shall be a document with tables represented as an Excel spreadsheet to include the functions, categories, sub-categories, references, etc. The output shall include an internal draft and a final document.

4.1.6. Cybersecurity Considerations for IoT Interagency Report (NISTIR)

The contractor shall facilitate the research, development, review, update, and comment resolution for the Cybersecurity Considerations for IoT Interagency Report. The NISTIR will be developed in collaboration with the NIST team and its content and findings will be driven by the research and documentation produced in the previous subtasks. The NISTIR shall include the following components:

- Survey of the different IoT industry Sectors/verticals
- Taxonomy for describing and classifying IoT
- Overlay of IoT functionality
- IoT cybersecurity threats, standards, guidelines, recommended practices, and regulations
- Mapping of the findings to the NIST Cybersecurity Framework and associated SP 800-53 security controls

The publication shall meet the NISTIR format, structure, and style. The comment resolution shall be a transparent, consensus-based process to address all public comments received on Draft NISTIR and include any updates based on public comments. The output shall include an internal draft, public draft, and WERB-ready final document.

4.2. PLANNING AND REPORTING - FFP

4.2.1. Kick-off Meeting

The contractor shall attend a kick-off meeting, on-site at NIST Gaithersburg or the Herbert Hoover Commerce Building in Washington, D.C. no later than 10 business days after award of the task order. The kick-off meeting shall be utilized to introduce all members of the contractor's team, review all task order requirements and deliverables, review the initial Project Work Plan provided by the contractor, evaluate the contractor's critical path analysis, and discuss the contractor's proposed approach. The contractor's key personnel shall be present at the kickoff meeting.

4.2.2. Integrated Project Work Plan

All work to be accomplished under this task order shall be managed through an Integrated Project Work Plan. NIST will approve the Project Work Plan or provide comments for revision within three (3) business days of delivery. The Project Work Plan must be statused monthly and sent to the project stakeholders, to include the Government Contracting Officer's Representative (COR), Technical Lead and Project Sponsor (optional), as well as the contractor's Task Order Manager and Key Personnel (optional) at least 3 days prior to the monthly status meeting. The Project Work Plan shall contain government dependencies highlighted in yellow. Updates to the plan that do not impact the critical path can be resolved at the monthly status meeting as a function of the project plan. Changes that extend the period

of performance or impact product delivery (i.e. removing PWS defined deliverables or adding new deliverables) will be addressed through mutually agreed upon contract modification action.

4.2.3. Regular status and reporting

The contractor Task Order Manager for this work effort shall attend a standing monthly Program Manager's meeting to provide a full status of the project to the government Program/Project Manager (P/PM), COR, and Project Sponsors. This meeting will typically be held on the NIST Gaithersburg campus, and will typically last for 1 to 2 hours per meeting. A conference room with a projection system will be provided for use by the contractors to present their updates. This meeting will be hosted by the P/PM for the contract (or their designee), and will typically be attended by the relevant government CORs, all relevant contractor PMs, and potentially government Tech Leads or Sponsors. A teleconference capability may be furnished if needed. At the discretion of the P/PM or COR, the contractor may be asked to conduct a monthly status meeting with the government technical leads and key personnel to resolve issues identified/presented at the standing monthly Program Manager's meeting. The contractor shall provide written impact statements for any event or circumstance that could impact the cost, schedule of project, or quality of the project work. Impact statements are due no later than 1 week after the monthly program status meeting. If during the program status meeting the government determines it is necessary to conduct a status meeting with a large contingent of stakeholders (i.e. project sponsors, technical leads, etc.), this meeting will be scheduled for two weeks from the monthly program status meeting, and the contractor will represent the status of the project and recommendations from the written impact statement(s).

After all tasks have been completed, the Contractor shall double check that all deliverables except the graphic have been uploaded to SharePoint. The graphic's source files shall be delivered on a CD or DVD.

THIS SPACE INTENTIONALLY LEFT BLANK

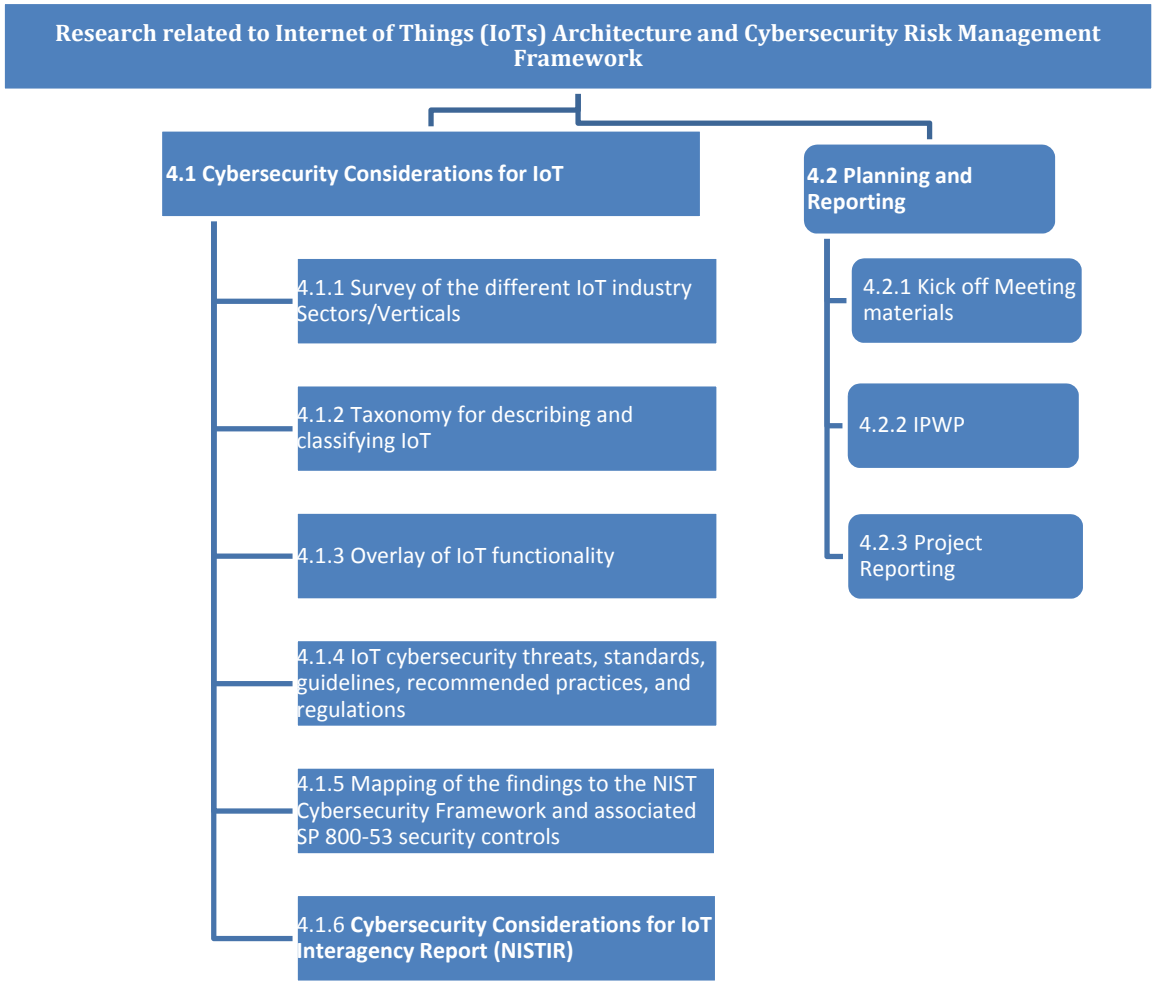

Figure 1 – Government Work Breakdown Structure (WBS)

5. DELIVERABLES

Task	Deliverable	Description	Media	Projected Completion Date
4.1.1	D1	Survey of the different IoT industry Sectors/verticals - Draft	MS Word, references links, documents, Web pages, etc.	As specified in COR-approved project work plan
4.1.1	D2	Survey of the different IoT industry Sectors/verticals - Final	MS Word, PowerPoint Presentation, references links, documents, Web pages, etc.	As specified in COR-approved project work plan
4.1.2	D3	Taxonomy for describing and classifying IoT - Draft	MS Word	As specified in COR-approved project work plan

4.1.2	D4	Taxonomy for describing and classifying IoT - Final	MS Word and PowerPoint Presentation	As specified in COR-approved project work plan
4.1.3	D5	Overlay of IoT Functionality - Draft	MS Word	As specified in COR-approved project work plan
4.1.3	D6	Overlay of IoT Functionality - Final	MS Word and PowerPoint Presentation	As specified in COR-approved project work plan
4.1.4	D7	IoT cybersecurity threats, standards, guidelines, recommended practices, and regulations - Draft	MS Word and MS Excel	As specified in COR-approved project work plan
4.1.4	D8	IoT cybersecurity threats, standards, guidelines, recommended practices, and regulations - Final	MS Word, MS Excel, and PowerPoint Presentation	As specified in COR-approved project work plan
4.1.5	D9	Mapping of the findings to the NIST Cybersecurity Framework and associated SP 800-53 security controls - Draft	MS Word and MS Excel	As specified in COR-approved project work plan
4.1.5	D10	Mapping of the findings to the NIST Cybersecurity Framework and associated SP 800-53 security controls - Final	MS Word, MS Excel, and PowerPoint Presentation	As specified in COR-approved project work plan
4.1.6	D11	Cybersecurity Considerations for IoT Interagency Report (NISTIR) – Annotated Outline	MS Word	As specified in COR-approved project work plan
4.1.6	D12	Cybersecurity Considerations for IoT Interagency Report (NISTIR) – Internal Draft	MS Word	As specified in COR-approved project work plan
4.1.6	D13	Cybersecurity Considerations for IoT Interagency Report (NISTIR) – Public Draft	MS Word	As specified in COR-approved project work plan
4.1.6	D14	Cybersecurity Considerations for IoT Interagency Report (NISTIR) – ERB-Ready final document	MS Word	As specified in COR-approved project work plan
4.2.1	D15	Kick-off meeting – Project Plan Review	MS Project / PDF	10 business days after award
4.2.2	D16	Integrated Project Work Plan	MS Word	Not more than 2 business days prior to Kick-off meeting
4.2.3	D17	Monthly Program Status Reporting	MS Word	Monthly at the contract program managers meeting.

All deliverables shall be provided to the COR and to the TPOC. All materials shall be submitted to NIST via electronic submission and hosted in a centralized repository. Currently, the centralized repository of record at NIST is SharePoint located at https://SharePoint.nist.gov.

6. PERFORMANCE REQUIREMENTS SUMMARY (PRS)

Desired Output			**Required Service**	
Internal draft posted to the NIST document repository. Final document and final presentation posted to the NIST document repository.			Research and document the findings	
Deliverable	Specific Task	Description	Performance Standard	Monitoring Method
1	4.1.1	Survey of the different IoT industry Sectors/verticals - Draft	Between 20 to 30 pages providing enough detail to demonstrate the understanding of the tasks. An example of a document is NISTIR 7904.	Tech Lead and COR review
2	4.1.1	Survey of the different IoT industry Sectors/verticals - Final	Between 20 to 30 pages giving enough details to demonstrate the understanding of the tasks. Between 10 to 15 slides for oral presentation in person or over collaborative environment portal. Shall incorporate NIST comments on previous deliverable.	Tech Lead and COR review
Desired Output			**Required Service**	
A logical and extendable taxonomy for describing IoT.			Research and document the results. Analysis. Taxonomy creation.	
Deliverable	Specific Task	Description	Performance Standard	Monitoring Method
3	4.1.2	Taxonomy for describing and classifying IoT - Draft	Between 7 to 15 pages giving enough details to demonstrate the understanding of the tasks.	Tech Lead and COR review
4	4.1.2	Taxonomy for describing and classifying IoT - Final	Between 7 to 15 pages giving enough details to demonstrate the understanding of the tasks. Between 7 to 10 slides for oral presentation in person or over collaborative environment portal. Shall incorporate NIST comments on previous deliverable.	Tech Lead and COR review
Desired Output			**Required Service**	
A document describing the sector specific reference model, the IoT architecture, the overlay and all associated information describing the mapping model.			Research and document the results. Analysis. Architecture and mapping creation.	
Deliverable	Specific Task	Description	Performance Standard	Monitoring Method

5	4.1.3	Overlay of IoT Functionality - Draft	Between 7 to 15 pages giving enough details to demonstrate the understanding of the tasks.	Tech Lead and COR review
6	4.1.3	Overlay of IoT Functionality - Final	Between 7 to 15 pages giving enough details to demonstrate the understanding of the tasks. Between 7 to 10 slides for oral presentation in person or over collaborative environment portal. Shall incorporate NIST comments on previous deliverable.	Tech Lead and COR review
Desired Output			**Required Service**	
A document that maps IoT architecture, components and functionalities to include specific capabilities and the security and privacy requirements that should be considered based on the understanding of the current threat landscape that drives the threat modeling exercise and countermeasures as prescribed by various national and international SDOs, government, and industry groups or consortiums.			Research and documenting results. Mapping creation. Analysis.	
Deliverable	Specific Task	Description	Performance Standard	Monitoring Method
7	4.1.4	IoT cybersecurity threats, standards, guidelines, recommended practices, and regulations - Draft	Between 7 to 10 pages giving enough details to demonstrate the understanding of the tasks. Between 100 to 150 rows of references threats, standards, guidelines, recommended practices, and regulations.	Tech Lead and COR review
8	4.1.4	IoT cybersecurity threats, standards, guidelines, recommended practices, and regulations - Final	Between 7 to 10 pages giving enough details to demonstrate the understanding of the tasks. Between 100 to 150 rows of references threats, standards, guidelines, recommended practices, and regulations. Between 10 to 15 slides for oral presentation in person or over collaborative environment portal. Shall incorporate NIST comments on previous deliverable.	Tech Lead and COR review
Desired Output			**Required Service**	
The contractor shall use the proposed countermeasures developed in the previous task to produce a security baseline targeted for each IoT class or technology grouping and sector. The output shall be a document with tables represented as an Excel spreadsheet to include the functions, categories, sub-categories, references, etc.			Research and documenting results. Security baseline creation. Analysis.	
Deliverable	Specific Task	Description	Performance Standard	Monitoring Method

9	4.1.5	Mapping of the findings to the NIST Cybersecurity Framework and associated SP 800-53 security controls - Draft	Between 7 to 10 pages giving enough details to demonstrate the understanding of the tasks. Between 200 to 300 rows of references functions, categories, sub-categories, framework implementation level.	Tech Lead and COR review
10	4.1.5	Mapping of the findings to the NIST Cybersecurity Framework and associated SP 800-53 security controls - Final	Between 7 to 10 pages giving enough details to demonstrate the understanding of the tasks. Between 200 to 300 rows of references functions, categories, sub-categories, framework implementation levels. Between 10 to 15 slides for oral presentation in person or over collaborative environment portal. Shall incorporate NIST comments on previous deliverable.	Tech Lead and COR review
Desired Output			**Required Service**	
A well-researched, logical Cybersecurity Considerations for IoT Interagency Report.			Document writing and editing. Comment tracking and resolution.	
Deliverable	Specific Task	Description	Performance Standard	Monitoring Method
11	4.1.6	Cybersecurity Considerations for IoT Interagency Report (NISTIR) – Annotated Outline	Approximately 5 – 12 pages in MS Word. Shall have a logical progression of topics based on previous deliverables.	Tech Lead and COR review
12	4.1.6	Cybersecurity Considerations for IoT Interagency Report (NISTIR) – Internal Draft	Between 52 to 80 pages in MS Word giving enough details to document the findings described in the previous subtasks. Between 100 to 150 rows of references threats, standards, guidelines, recommended practices, and regulations. Between 200 to 300 rows of references functions, categories, sub-categories, framework implementation levels. Shall incorporate NIST comments on previous deliverable.	Tech Lead and COR review
13	4.1.6	Cybersecurity Considerations for IoT Interagency Report (NISTIR) – Public Draft	Between 52 to 80 pages giving enough details to document the findings described in the previous subtasks. Between 100 to 150 rows of references threats, standards, guidelines, recommended practices, and regulations. Between 200 to 300 rows of references functions, categories, sub-categories, framework implementation levels. Shall incorporate NIST comments on previous deliverable. It is expected that the amount of new material at this stage will not be significant.	Tech Lead and COR review

14	4.1.6	Cybersecurity Considerations for IoT Interagency Report (NISTIR) – ERB-Ready final document	Between 52 to 80 pages giving enough details to document the findings described in the previous subtasks. Between 100 to 150 rows of references threats, standards, guidelines, recommended practices, and regulations. Between 200 to 300 rows of references functions, categories, sub-categories, framework implementation levels. Shall incorporate NIST comments on previous deliverable. It is expected that the amount of new material at this stage will not be significant.	Tech Lead and COR review
Desired Output			**Required Service**	
Efficient, accurate project management			A well-organized project initiation and execution, with sound management of contract resources, and timely deliverables of professional quality.	
Deliverable	Specific Task	Description	Performance Standard	Monitoring Method
15	4.2.1	Kick-off Meeting agenda and materials - Contractor shall supply an agenda for the meeting as well as relevant information on contractor staff.	Electronic copy of the agenda should be delivered to the COR at least 2 business days before the meeting.	Tech Lead and COR review
16	4.2.2	Integrated Project Work Plan	The IPWP will be delivered no later than 2 business days before the Kick-off Meeting. The IPWP shall include an identification of contractor resources, deliverables and completion dates, sequence of events, start dates, and duration for each activity. The IPWP will be available in electronic format.	Tech Lead and COR review
17	4.2.3	Monthly Program Status Reporting	Complete information available on program status delivered in a clear format.	

7. CONTRACTOR MINIMUM REQUIREMENTS

Contractor Key Personnel shall meet the following minimum qualifications for each of the respective required key personnel positions. The title of the labor categories (LCATs) given below are taken from the IDIQ list of required labor categories.

7.1. TECHNICAL SUBJECT MATTER SPECIALIST (SENIOR)

Minimum/General Experience:

This position requires 12 years of intensive and progressive experience in the applicable specialty field or, if the subject matter is less than 10 years old, the position requires being involved in the subject matter since the inception of the subject matter.

Functional Responsibilities: Duties may include but are not limited to: Applies subject matter knowledge to high level analysis, collection, assessment, design, development, modeling, simulation, integration,

installation, documentation, and implementation. Resolves problems, which require an intimate knowledge of the related technical subject matter. Applies principles and methods of the subject matter to specialized solutions. Includes but not limited to; identity management, biometrics, industrial controls, electronic voting, cloud computing, cyber security, cryptography, virtualization, PKI, XML, applied IT policy and compliance, networking, business processes, security automation, and logistical support activities.

Minimum Education: A Bachelor's degree with a curriculum or major field of study which is closely related to the work to be accomplished, and/or in a computer science, information system, engineering, or a mathematics-intensive discipline. OR a Master's Degree (in subjects described above) with 9 years of applicable experience in a field closely related to and applicable to the task order. OR a PhD degree (in subjects described above) with 6 years of applicable experience. OR no degree and 16 years of intensive and progressive experience in the applicable specialty field.

Specialty Knowledge: This task order requires specialty knowledge in IoT, cybersecurity controls, the NIST Cybersecurity Framework, SP 800-53 Rev 4, and taxonomies. This task order will also require some technical writing expertise.

7.2. PROGRAM MANAGER 2 – TASK ORDER LEVEL

Minimum/General Experience:

This position requires a minimum of 6 years' general project management experience and 3 years IT experience in computer security. Experience includes increasing responsibilities in information systems design and management.

Functional Responsibilities: Duties may include but are not limited to: Serves as project manager for a large, complex task order and shall assist the Program Manager in working with the ordering activity Contracting Officer (CO), the Federal Acquisitions Contract – Project/Program Manager (FAC-P/PM), the contract-level Contracting Officer's Representative (COR), and the task order-level COR(s), ordering activity management personnel and customer agency representatives. The Project Manager is responsible for the overall management of the specific task order(s) and insuring that the technical solutions and schedules in the task order are implemented in a timely manner. Performs enterprise wide horizontal integration planning and interfaces to other functional systems.

Minimum Education: Must either be certified as a.) Project Management Professional (PMP) by the Project Management Institute (PMI) or other such credentialing organization, or b.) Have been or currently are certified as a FAC- Program/Project Manager (P/PM) (Mid or Senior level). A Defense Systems Management College (DSMC) Program Management (PM) certification of Level 2 or 3 will be considered equivalent to a FAC-P/PM Mid or Senior Level. A Bachelor's degree in computer science/engineering technology, software/programming, or mathematics can be substituted for 2 years' general experience and 2 years IT experience. A PhD or Master's Degree (in subjects described above) can be substituted for 3 years IT experience. A Master's Degree in Project Management can be substituted for 3 years' project management experience.

8. TRAVEL

No travel is required for this task order.

9. PLACE OF PERFORMANCE

The majority of the work shall be performed at the Contractor's site, although meetings may be conducted at NIST or at other local agreed-upon sites.

10. PERIOD OF PERFORMANCE

The period of performance of this task order is 12 months from award.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu