SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE	OF
OCIO-20-0100	1	61

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
31310020C0015	09/01/2020			

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	JOHNNIE BAKER		

9. ISSUED BY — CODE NRCHQ

US NRC - HQ
ACQUISITION MANAGEMENT DIVISION
MAIL STOP TWFN-07B20M
WASHINGTON DC 20555-0001

10. THIS ACQUISITION IS ☐ UNRESTRICTED OR ☒ SET ASIDE: 100.00 % FOR:

☐ SMALL BUSINESS
☐ HUBZONE SMALL BUSINESS
☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
☐ EDWOSB
☒ 8(A)

NAICS: 541511

SIZE STANDARD: $30.0

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED ☐ SEE SCHEDULE	12. DISCOUNT TERMS	☐ 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING / 14. METHOD OF SOLICITATION
	30		☐RFQ ☐IFB ☐RFP

15. DELIVER TO — CODE NRCHQ

NUCLEAR REGULATORY COMMISSION
NUCLEAR REGULATORY COMMISSION
WASHINGTON DC 20555-0001

16. ADMINISTERED BY — CODE NRCHQ

US NRC - HQ
ACQUISITION MANAGEMENT DIVISION
MAIL STOP TWFN-07B20M
WASHINGTON DC 20555-0001

17a. CONTRACTOR/ OFFEROR — CODE 838011740 — FACILITY CODE

CODE PLUS INC
ATTN JINAN ABOUSHAKRA
2750 PROSPERITY AVENUE
SUITE 230
FAIRFAX VA 220314338

TELEPHONE NO. 7038460030101

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY — CODE NRCPAYMENTS

FISCAL ACCOUNTING PROGRAM
ADMIN TRAINING GROUP AVERY STREET A3-G
BUREAU OF THE FISCAL SERVICE
PO BOX 1328
PARKERSBURG WV 26106-1328

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Period of Performance: 09/01/2020 to 08/31/2021 SBA Requirement Number: 0353/20/0778				
00001	BASE AND EXERCISED OPTIONS Computer Security Incident Response Team (CSIRT) For Cyber Control and Incident Response (CCIR) FFP Accounting Info: 2020-X0200-FEEBASED-10-10D011-6182-51-J-145-252A-5 Continued ...				[redacted]

(Use Reverse and/or Attach Additional Sheets as Necessary)

25. ACCOUNTING AND APPROPRIATION DATA
See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)* [redacted]

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED.
☒ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☒ ARE ☐ ARE NOT ATTACHED.

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

☐ 29. AWARD OF CONTRACT: _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
	Dominique C. Malone

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
		DOMONIQUE MALONE	08/24/2020

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	1-J-145-6182 Funded: [redacted] Accounting Info: 2020-X0200-FEEBASED-10-10D011-6182-51-J-144-2574-5 1-J-144-6182 Funded: [redacted] Accounting Info: 2020-X0200-FEEBASED-10-10D010-6182-51-J-145-2574-5 1-J-145-6182 Funded: [redacted] Accounting Info: 2020-C0200-FEEBASED-10-10D011-6166-34-5-144-2574-3 4-5-144-6166 Funded:[redacted] Accounting Info: 2020-X0200-FEEBASED-10-10D011-6166-17-4-144-2574-1 7-4-144-6166 Funded: [redacted]				
10001	OPTION YEAR 1 Computer Security Incident Response Team (CSIRT) For Cyber Control and Incident Response (CCIR) Amount: [redacted] (Option Line Item) TASKS: C4.10 Support for NRC Network Data Loss Continued ...				0.00

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
	32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	37. CHECK NUMBER
☐ PARTIAL ☐ FINAL			☐ COMPLETE ☐ PARTIAL ☐ FINAL	

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Prevention Appliance and IRDB Application C4.3 Maintain and Operate the Network Data Loss Prevention Appliance C4.2 Analyze Computer Security Incident Response for Tier 1 C4.1 Maintain, Modify and Enhance the Cyber Security System/Application of the IRDB C4.8 Provide Tier 1 Support for Quarterly Phishing Tests of NRC End User C4.9 Provide Project Management Support C4.7 Perform Bi-annual Incident Response Testing C4.7 Perform Bi-annual Incident Response Testing				
10002	OPTION YEAR 1 OPTIONAL TASKS FOR Computer Security Incident Response Team (CSIRT) For Cyber Control and Incident Response (CCIR) Amount: [redacted] (Option Line Item) TASKS: C4.6 Identify and Analyze Cyber Security Process and Assessment Documentation C4.5 Monitor Cyber Security of Internal and Outbound Threat Vectors C4.4 Develop and Submit Reports on Cyber Security Situational Awareness				0.00
20001	OPTION YEAR 2 Computer Security Incident Response Team (CSIRT) For Cyber Control and Incident Response (CCIR) Amount: [redacted] (Option Line Item) TASKS: C4.10 Support for NRC Network Data Loss Prevention Appliance and IRDB Application C4.3 Maintain and Operate the Network Data Loss Prevention Appliance C4.2 Analyze Computer Security Incident Response for Tier 1 C4.1 Maintain, Modify and Enhance the Cyber Security System/Application of the IRDB C4.8 Provide Tier 1 Support for Quarterly Phishing Tests of NRC End User C4.9 Provide Project Management Support C4.7 Continued ...				0.00

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Perform Bi-annual Incident Response Testing C4.7 Perform Bi-annual Incident Response Testing				
20002	OPTION YEAR 2 OPTIONAL TASKS FOR Computer Security Incident Response Team (CSIRT) For Cyber Control and Incident Response (CCIR) Amount: [redacted] (Option Line Item) TASKS: C4.6 Identify and Analyze Cyber Security Process and Assessment Documentation C4.5 Monitor Cyber Security of Internal and Outbound Threat Vectors C4.4 Develop and Submit Reports on Cyber Security Situational Awareness				0.00
30001	OPTION YEAR 3 Computer Security Incident Response Team (CSIRT) For Cyber Control and Incident Response (CCIR) Amount: [redacted] (Option Line Item) TASKS: C4.10 Support for NRC Network Data Loss Prevention Appliance and IRDB Application C4.3 Maintain and Operate the Network Data Loss Prevention Appliance C4.2 Analyze Computer Security Incident Response for Tier 1 C4.1 Maintain, Modify and Enhance the Cyber Security System/Application of the IRDB C4.8 Provide Tier 1 Support for Quarterly Phishing Tests of NRC End User C4.9 Provide Project Management Support C4.7 Perform Bi-annual Incident Response Testing C4.7 Perform Bi-annual Incident Response Testing				0.00
30002	OPTION YEAR 3 OPTIONAL TASKS FOR Computer Security Incident Response Team (CSIRT) For Cyber Control and Incident Response (CCIR) Amount: [redacted] (Option Line Item) Continued ...				0.00

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	TASKS: C4.6 Identify and Analyze Cyber Security Process and Assessment Documentation C4.5 Monitor Cyber Security of Internal and Outbound Threat Vectors C4.4 Develop and Submit Reports on Cyber Security Situational Awareness				
40001	OPTION YEAR 4 Computer Security Incident Response Team (CSIRT) For Cyber Control and Incident Response (CCIR) Amount: [redacted] (Option Line Item)				0.00
	TASKS: C4.10 Support for NRC Network Data Loss Prevention Appliance and IRDB Application C4.3 Maintain and Operate the Network Data Loss Prevention Appliance C4.2 Analyze Computer Security Incident Response for Tier 1 C4.1 Maintain, Modify and Enhance the Cyber Security System/Application of the IRDB C4.8 Provide Tier 1 Support for Quarterly Phishing Tests of NRC End User C4.9 Provide Project Management Support C4.7 Perform Bi-annual Incident Response Testing C4.7 Perform Bi-annual Incident Response Testing				
40002	OPTION YEAR 4 OPTIONAL TASKS FOR Computer Security Incident Response Team (CSIRT) For Cyber Control and Incident Response (CCIR) Amount: [redacted] (Option Line Item)				0.00
	TASKS: C4.6 Identify and Analyze Cyber Security Process and Assessment Documentation C4.5 Monitor Cyber Security of Internal and Outbound Threat Vectors C4.4 Develop and Submit Reports on Cyber Security Situational Awareness				
	The obligated amount of award: [redacted]. The total for this award is shown in box 26.				

SECTION B - Supplies or Services/Prices

B.1 BRIEF PROJECT TITLE AND WORK DESCRIPTION

(a) The title of this project is: Computer Security Incident Response Team (CSIRT) For Cyber Control and Incident Response (CCIR) Services 8(a)

(b) Summary work description: The Contractor shall support CSIRT in developing, establishing and maintaining a robust cyber security program that includes, but is not limited to, the IT Security Service domain requirements. The Contractor shall provide support services in operational cyber security. This includes the following:

1. Maintain, modify and enhance the Cyber Security System/Application of the Incident Response Database (IRDB)
2. Analyze computer security incident response for Tier 1
3. Maintain and operate the Data Loss Prevention Appliance
4. Develop and submit reports on Cyber Security Situational Awareness
5. Monitor cyber security of internal and outbound threat vectors
6. Identify and analyze Cyber Security Process and Assessment Documentation
7. Perform bi-annual Incident Response Testing
8. Provide Tier 1 support for Quarterly Phishing Tests of NRC End Users
9. Provide project management support
10. Support for NRC Security Tools including IRDB Application

(End of Clause)

B.2 CONSIDERATION AND OBLIGATION-FIRM-FIXED-PRICE

The total amount of the Firm-Fixed-Price portion of this contract is $776,330.04, and this amount is fully-funded.

(End of Clause)

B.3 PRICE/COST SCHEDULE

ITEM	DESCRIPTION / TASKS	POP	QTY	UNIT	UNIT PRICE	TOTAL
00001	BASE CSIRT For CCIR. Includes all tasks C.3.1 - C.3.11	09/01/2020 – 08/31/2021	12	Month	[redacted]	[redacted]
10001	OPTION YEAR 1 CSIRT For CCIR. Includes Tasks C.3.1,C.3.2,C.3.3,C.3.7,C.3.8,C.3.9,C.3.10	09/01/2021 – 08/31/2022	12	Month	[redacted]	[redacted]
10002	OPTION YEAR 1 OPTIONAL TASKS FOR CSIRT For CCIR. Includes Tasks C.3.4,C.3.5,C.3.6	09/01/2021 – 08/31/2022	12	Month	[redacted]	[redacted]

20001	OPTIOIN YEAR 2 CSIRT For CCIR. Includes Tasks C.3.1,C.3.2,C.3.3,C.3.7,C.3.8,C.3.9,C.3.10	09/01/2022 – 08/31/2023	12	Month	[redacted]	[redacted]
20002	OPTION YEAR 2 OPTIONAL TASKS FOR CSIRT For CCIR. Includes Tasks C.3.4,C.3.5,C.3.6	09/01/2022 – 08/31/2023	12	Month	[redacted]	[redacted]
30001	OPTION YEAR 3 CSIRT For CCIR. Includes Tasks C.3.1,C.3.2,C.3.3,C.3.7,C.3.8,C.3.9,C.3.10	09/01/2023 – 08/31/2024	12	Month	[redacted]	[redacted]
30002	OPTION YEAR 3 OPTIONAL TASKS FOR CSIRT For CCIR. Includes Tasks C.3.4,C.3.5,C.3.6	09/01/2023 – 08/31/2024	12	Month	[redacted]	[redacted]
40001	OPTION YEAR 4 CSIRT For CCIR. Includes Tasks C.3.1,C.3.2,C.3.3,C.3.7,C.3.8,C.3.9,C.3.10	09/01/2024 – 08/31/2025	12	Month	[redacted]	[redacted]
40002	OPTION YEAR 4 OPTIONAL TASKS FOR CSIRT For CCIR. Includes Tasks C.3.4,C.3.5,C.3.6	09/01/2024 – 08/31/2025	12	Month	[redacted]	[redacted]
					TOTAL:	[redacted]

SECTION C - Description/Specifications

C.1 STATEMENT OF WORK

DESCRIPTION/SPECIFICATIONS/WORK STATEMENT

Contents

DESCRIPTION/SPECIFICATIONS/WORK STATEMENT

C.1 Background

The Nuclear Regulatory Commission (NRC) was created as an independent Agency by Congress in 1974 to enable the nation to safely use radioactive materials for beneficial civilian purposes while ensuring that people and the environment are protected. It regulates commercial nuclear power plants and other uses of nuclear materials, such as in nuclear medicine, through licensing, inspection and enforcement of its requirements. The NRC's headquarters are in Rockville, Maryland, and the NRC has regional offices in King of Prussia, Pennsylvania; Atlanta, Georgia; Lisle, Illinois; Arlington, Texas, and the Technical Training Center (TTC) in Chattanooga, Tennessee.

The NRC's Computer Security Incident Response Team (CSIRT) within the Office of the Chief Information Officer (OCIO) is the focal point for receiving, tracking, monitoring, and reporting NRC's computer security incidents; maintaining an awareness of the threat to NRC's IT infrastructure; and providing appropriate information to senior NRC officials so that they maintain an up-to-date awareness of cyber threats and NRC's vulnerability. CSIRT also performs the following: Tier 1 analysis and triage of suspicious emails; monitoring of the NRC network data loss prevention (DLP) appliance; trend analysis of suspicious email and DLP events; and recommending actions to minimize or prevent unauthorized releases of agency information. CSIRT also communicates relevant

computer security information such as security alerts, advisories, and bulletins to NRC staff, and acts as the reporting authority to the US Computer Emergency Readiness Team (CERT), the Office of Management and Budget (OMB), law enforcement, and criminal investigation groups for cyber-related attacks against the NRC. CSIRT also performs annual agency wide Incident Response testing, maintains network Data Loss Prevention (DLP) appliance capabilities, and reports findings daily, weekly and monthly.

C.2 Objective

The Contractor shall support CSIRT in developing, establishing and maintaining a robust cyber security program that includes, but is not limited to, the IT Security Service domain requirements. The Contractor shall provide support services in operational cyber security. This includes the following:

1. Maintain, modify and enhance the Cyber Security System/Application of the Incident Response Database (IRDB)
2. Analyze computer security incident response for Tier 1
3. Maintain and operate the Data Loss Prevention Appliance
4. Develop and submit reports on Cyber Security Situational Awareness
5. Monitor cyber security of internal and outbound threat vectors
6. Identify and analyze Cyber Security Process and Assessment Documentation
7. Perform bi-annual Incident Response Testing
8. Provide Tier 1 support for Quarterly Phishing Tests of NRC End Users
9. Provide project management support
10. Support for NRC Security Tools including IRDB Application

C.3 Scope of Work/Tasks

The Contractor shall provide all personnel necessary to accomplish the tasks and deliverables described in this Statement of Work (SOW).

C.3.1 Maintain, Modify and Enhance the Cyber Security System/Application of the Incident Response Database (IRDB)

The Contractor shall maintain, modify, and enhance the IRDB application and generate, modify, and create reports on the IRDB. The Contractor shall have knowledge of and the ability to add, modify, and delete fields to the application. The IRDB has an average of 1 major and 3 minor upgrades per year and requires ongoing maintenance.

C.3.2 Analyze Computer Security Incident Response for Tier 1

The Contractor shall analyze suspicious emails, email senders, and notifications from users. The Contractor shall create and distribute the monthly CSIRT watch officer schedule, carry the incident response telephone, and be on call 24/7 to answer calls and respond to incidents. The Contractor shall respond to users within the Data Loss Prevention application and communicate with the Security Operations Center (SOC) and other NRC Information Security (InfoSec) personnel on any trends as well as computer security concerns. The Contractor shall provide Tier 1 analysis and triage of suspicious emails and, if applicable, create computer security incidents. If the Contractor's analysis deems that the suspect data is malicious, then the Contractor shall create a record of

those incidents. Within 24 hours the Contractor shall then categorize the various threats and threat vectors, enter it into the IRDB, and CSIRT assigns tickets within the agency IT service management system for other technical teams to conduct further investigations. As a historical reference and for planning purposes, the NRC creates approximately 500 computer security incidents per year.

C.3.3 Maintain and Operate the Network Data Loss Prevention Appliance

The Contractor shall use the Agency's Network Data Loss Prevention (DLP) platform to perform security monitoring of the NRC internal email traffic, internet connections, and web domain interfaces and identify and report on threats in the IRDB. The Contractor shall upgrade and maintain the DLP appliances, configure, and modify the policies/rules following COR approval, and act as the system administrator. The Contractor shall assist in any controls that need to be implemented. Additionally, the Contractor shall perform Tier 1 email and phishing incident response on logs and alerts identified by the network DLP appliance and shall leverage their corporate phishing attack attribution service to provide additional reporting depth and analysis to their findings. The network DLP has an average of 1 major and 3 minor upgrades per year and requires ongoing maintenance.

C.3.4 Develop and Submit Reports on Cyber Security Situational Awareness

The Contractor shall perform Cyber Security Metrics Reporting in support of CSIRT situational awareness tracking and reporting using the IRDB and other reporting tools as provided for by the Government. The Contractor shall deliver monthly, quarterly and annual incident report statistics and other reporting criteria as required by CSIRT or external entities such as the U.S. Government Accountability Office (GAO) or OMB. In addition, the Contractor shall provide monthly reporting to the COR of the IRDB incident totals and other statistics for other reports like Cyberscope, Federal Information Technology Acquisition (FITARA) or the Cyber security dashboard. In addition, the Contractor shall provide reports, per COR request, such as Network DLP reports, which are typically required 3 days a week for management security meetings. The Contractor shall be responsible for updating, maintaining and performing the Cyber Security Event – Rapid Response Plan.

C.3.5 Monitor Cyber Security of Internal and Outbound Threat Vectors

The Contractor shall perform security monitoring of the internal and email networks using the Network DLP appliance and identify and report on security threats based on logs and alerts. The Contractor shall use the network DLP platform and create Remedy tickets. Additionally, the Contractor shall perform email and phishing incident response and shall leverage their corporate phishing attack attribution service to provide additional reporting depth and analysis to their findings.

C.3.6 Identify and Analyze Cyber Security Process and Assessment Documentation

The Contractor shall create and provide technical documentation, which includes, but is not limited to, security authorization process artifacts, cyber security capability assessments, and recommendations to improve agency cyber security. The Contractor

shall document, capture, and report on the security posture of the agency and document cyber situational awareness security capabilities based on IRDB records, resolutions and statistics. The Contractor shall also provide documentation of internal cyber situational awareness, analysis and response processes, procedures and policy recommendations to record and sustain cyber situational awareness. The Contractor shall provide input into a Cyber Security Metrics dashboard that reflects cyber security incidents and real-time cyber security status and ad hoc reports. The Contractor shall update one Standard Operating Procedure, Plan, and Policy (SOP) document per year and update input into the Cyber Security Metrics dashboard 12 times per year.

C.3.7 Perform Bi-annual Incident Response Testing

The Contractor shall formulate the Bi-annual agency-wide Incident Response Test Plan, run the required tests, and gather and report on the test results in the required format listed under the Deliverable table (see C.7). The Contractor shall create and conduct the bi-annual test plan (i.e., 2 test plans per year) and provide two (2) test result reports per year.

C.3.8 Provide Tier 1 Support for Quarterly Phishing Tests of NRC End User

The Contractor shall record the results of the quarterly Phishing test sent to all NRC users. The Contractor shall respond to the NRC end users in the tests and create test result reports. The agency performs four (4) tests per year and the Contractor shall provide 4 test reports per year to the COR.

C.3.9 Provide Project Management Support

The project manager shall be responsible for the deliverables listed in Section C.7 (List of Deliverables) and manage all Contractor tasks and deliverables as well as submit and verify Contractor invoices. The Project Manager shall be required to attend various meeting and coordinate efforts with the COR and other Government personnel. The Contractor shall provide status reports including self-evaluations and management briefings to document support service activities. The Contractor shall summarize accomplishments, present analyses of major challenges, and offer innovative solutions to improve weaknesses based on feedback provided by the COR.

C.3.10 Support for NRC Security Tools including IRDB Application

The Contractor shall, in close collaboration with the CSIRT and other NRC vendors who support the Network and SOC teams, install, configure, maintain and operate the current versions of the network data loss prevention appliances to assure they are running optimally, efficiently and effectively. Typical actions required include, but are not limited to the following: monitoring and operating the appliances; reporting on alerts and findings; recommending improvements to processes and use cases; evaluating and recommending mechanisms and approaches for allowing the network data loss prevention appliance to observe lateral information movement within the enterprise (i.e., permitting views into exfiltration staging and providing packet capture for information not traversing the perimeter); evaluating, designing and recommending security orchestration capabilities to allow for immediate and continuous detection and responses across the enterprise (based on centralized logging within NRC); recommending

outbound buffering and blocking capabilities within the various programs; recommending outbound detection and enforcement for key words, concepts, phrases and data patterns; managing and maintaining the user lists (create, modify and delete user accounts as requested); applying security patches to the application; plan, test and deploy application patches; troubleshoot/escalate problems with the support vendor; assure backups are performed to allow for efficient system restore in the event of data corruption or loss. Note: for the IRDB application these tasks are primarily performed by the NRC Data Center Operations Teams who maintain the server and operating system; however, the Contractor shall provide assistance for any work that is required by the COR related to data corruption or loss. In addition, the Contractor shall adhere to all NRC processes and procedures (for example, following the NRC Change Management process), perform front-end server application maintenance such as document existing processes, workflows and settings, password resets, account lockouts and modifications to allow compliance with US-CERT requirements. In addition, the Contractor shall perform back-end server maintenance support functions such as documenting application changes to the IRDB and network data loss prevention applications, reviewing application logs or coordinating the utilization of NRC's log management system, and providing recommendations for enhancements or modifications in policies, rules, and content. The Contractor shall conduct in-depth troubleshooting of application problems and assure the application is running optimally. The estimated level of effort for this task is anticipated to be up to 1000 hours per year.

C.3.11 Technical Kickoff Meeting

The Contractor shall hold a technical kickoff meeting within ten (10) business days following contract award. The Project Manager and a technical lead person shall attend in person and present for review and approval by the COR, the details of the intended contract approach, work plan, and the plan for staffing the contract. Following the kickoff meeting, the Contractor shall electronically submit to the COR the kickoff presentation slides within 5 business days after the kickoff meeting, which shall include any COR-requested changes.

C.4 Labor Roles, Key Personnel and Levels of Effort

Labor Roles, Requirements and Key Personnel.

The Project Manager shall have a minimum requirement of a Project Management Professional certification.

All other Contractor personnel working under this contact shall meet the minimum requirements for experience and education, as follows:

The Contractor's personnel shall have an in-depth understanding and 2 + years of professional experience in using some of the following tools listed below, including but not limited to:

• Information Assurance Applications: Fidelis, RSA Archer Incident Management and others as acquired or deployed by the NRC.

• Security Expertise: computer and network forensics, secure baseline configurations,

network engineering, network monitoring, Intrusion Detection Systems (IDS), log capture and edit, Firewalls, Virtual Private Networking (VPN), network routers, switches and infrastructure, Wireless network technologies (802 .11x, Bluetooth) as well as Citrix, Mobility Solutions, Malware, and Spyware.

• Operating systems: VMware, Linux, Solaris, Microsoft Windows, Microsoft Windows Servers, Microsoft Office 365. Contractors should also have an understanding and a level of experience working with virtualization techniques and operating system images.

• Software Applications: SQL, Exchange, Microsoft Internet Information Services (IIS), Oracle, and Citrix.

Contractor personnel shall keep current with advances in relevant technology and share this knowledge with other Contractor and Government NRC personnel. Contractor personnel shall act in a consultative manner, proactively search for creative solutions and strategies, respond promptly, professionally and courteously to Government requests for recommendations on in-scope NRC cybersecurity topics, and freely provide knowledge transfer of work products and technology expertise.

The role that is defined as key personnel is the part-time Project Manager. Note: the minimum requirements for the following roles are listed above and position duties are listed below:

Role	Position Duties	Key Personnel* (yes or no)
Information Assurance Development Engineer	Analyzes and defines security requirement for computer systems which may include servers, network appliances and workstations. Designs, develops, engineers, and implements solutions that meet security requirements. Provides integration and implementation of the computer system security solution.	no
Information Assurance Systems/Network Specialist	Analyzes general information assurance-related technical problems and provides basic engineering and technical support in solving these problems. Designs, develops, engineers, and implements solutions that meet network security requirements. Performs vulnerability/risk analyses of computer systems and applications during all phases of the system development life cycle.	no
Data Security Analyst - Intermediate	Interfaces with user community to understand security needs and implements procedures to accommodate them. Conducts accurate evaluation of the level of security required. Provides management with status reports.	no

Security Coordinator	Coordinates, develops, and evaluates security programs for an organization and authors documents.	no
Project Manager	Responsible for all aspects of the development and implementation of assigned projects and is the single point of contact for those projects. Takes projects from original concept through final implementation. Interfaces with all areas affected by the project including end users, computer services and client services.	yes

*See NRCAR 2052.215-70, “Key Personnel”

C.5 Certification and License Requirements

The Contractor is responsible for ensuring that one or more of the employees assigned to this Government contract possess and maintain the following professional certification:

- Certified Information Systems Security Professional (CISSP)
- Project Management Professional (PMP)

C.6 Reporting Requirements

C.6.1 Bi-Weekly Reports

The Contractor shall also provide a bi-weekly status report in a format similar to the monthly report. The bi-weekly status report shall include the following: contract summary information, work completed during the specified period, milestone schedule information, problem resolution, and staff hour summary. Each report shall include the following for each discrete task:

(a) A listing of the efforts completed during the period, and milestones reached or, if missed, an explanation provided;

(b) Any problems or delays encountered or anticipated and recommendations for resolution. If the recommended resolution involves a contract modification, e.g., change in work requirements, level of effort (cost) or schedule delay, the Contractor shall submit a separate letter in writing to the contracting officer identifying the required change and estimated cost impact and set up a meeting;

(c) A summary of progress to date; and

(d) Plans for the next reporting period.

C.6.2 Bi-Weekly Project Plan/Milestone Schedule

The Contractor shall develop and maintain a Project Plan and provide electronic copies of the Project Plan to the NRC COR bi-weekly with the bi-weekly status report.
The Project Plan shall specify a milestone schedule and the resources/staff needed to

complete the work.

C.6.3 Ad Hoc Documents and Reports
The Contractor shall be tasked by the COR to provide various technical documents and reports as described above under sections C.4.4 and C.4.6.

C.6.4 Final Report
The Contractor shall provide a final report summarizing the work performed and the results and conclusions under this contract/order.

C.7 List of Deliverables

The Contractor shall submit the following deliverables electronically to the COR.

Section #	Deliverable	Due Date	Format	Submit to
C.3.11	Kickoff Meeting Presentation	No Later than (NLT) 5 business days following the kickoff meeting	PowerPoint or other COR-approved format	COR
C.3.4 C.3.6	Weekly, monthly, quarterly and annual incident reports; Rapid Response Plan; SOP	To be determined subsequent to contract award	Word Document	COR
C.3.7	Bi-Annual Incident Result Test Plan and Test Result Report	NLT end of Q2 (March 31) and Q4 (September 30) each year	Word Document	COR
C.3.8	Phishing Results Report	Quarterly	Word Document and Excel	COR
C.6.1 and C.6.2	Bi-Weekly Project Plan/Milestone Schedule and Bi-Weekly Report	NLT 15th of the following month	Word Document	COR
C.6.3	Ad Hoc Documents and Reports	as required by COR	Word Document	COR
C.6.4	Final report	NLT 30 days prior to contract expiration	Word Document	COR

C.8 Required Materials/Facilities

Not Applicable

C.9 Release of Publications

Any documents generated by the Contractor under this contract shall not be released for publication or dissemination without CO and COR prior written approval.

C.10 Place of Performance

The work to be performed under this contract shall be primarily performed at NRC Headquarters located at 11545 Rockville Pike, Rockville, MD 20852.

C.11 Recognized Holidays

Contractor personnel shall not be required to perform onsite on the Federal holidays identified below. Contractor personnel shall comply with their company's policies and procedures regarding their work status on these days:

New Year's Day	Labor Day
Martin Luther King Jr.'s Birthday	Columbus Day
President's Day	Veteran's Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

C.12 Hours of Operation

The Contractor shall provide required support either on site or via telework as determined by the COR within the range of hours, starting no earlier than 8:00 AM and ending no later than 7:00 PM, Monday thru Friday, except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor shall, at all times, maintain an adequate workforce for the uninterrupted performance of all tasks defined within this SOW when the Government facility is not closed for the above reasons. When hiring personnel, the Contactor shall keep in mind that the stability and continuity of the workforce are essential. The project manager shall be on call 24/7 to provide support.

C.13 Contractor Travel

Not applicable, as local travel to the NRC is the responsibility of the Contractor.

C.14 Data Rights

The NRC shall have unlimited rights to, and ownership of, all deliverables provided under this contract/order, including reports, recommendations, briefings, work plans and all other deliverables. All documents and materials, to include the source codes of any software, produced under this contract/order are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials shall not be used or sold by the Contractor without prior written authorization from the COR. All materials supplied to the Government shall be

the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

C.15 Incremental Development for Software

Not Applicable

C.16 Section 508 – Information and Communication Technology Accessibility

Not Applicable

C.17 Applicable Publications (Current Editions)

The Contractor shall comply with the following applicable regulations, publications, manuals, and local policies and procedures.

The Contractor shall have knowledge and experience with, but not limited to, the following federal regulations, standards and guidelines, and their most recent version:

- The Federal Information Security Management Act of 2002 and 2014
- The E-Government Act of 2002
- The Clinger-Cohen Act of 1996
- The Financial Management Improvement Act of 1996
- The Financial Management Integrity Act of 1982
- The Privacy Act of 1974
- Federal Enterprise Architecture (FEA)
- Cyber Security relevant OMB Memorandums
- OMB Circulars
- Presidential Directives
- Department of Homeland Security - USCERT Incident Response Directives
- National Security Directives
- Executive Orders
- Intelligence Reform and Terrorism Prevention Act
- Director of Central Intelligence Directives
- NIST Federal Information Processing Standards (FIPS)
- NIST SP 800 series
- CNSS publications
- NIST Guide for Information Security Program Assessments and System Reporting Form
- Department of Homeland Security National Strategy to Secure Cyberspace

C.18 Security Requirements

Contractor personnel shall be required to return NRC issued Personal Identification Verification (PIV) cards/badges to the COR at the end of the contract period of performance. If the contractor's personnel voluntarily leaves the company, the badge shall be returned on the personnel's final day of employment. Once the badge is returned to the NRC, the contractor personnel will no longer have access to NRC buildings, sensitive automated information technology systems or data. Additional information related to the returning of PIV badges can be found in Management Directive 12.1, Section 5.

SECTION D - Packaging and Marking

D.1 PACKAGING AND MARKING

(a) The Contractor shall package material for shipment to the NRC in such a manner that will ensure acceptance by common carrier and safe delivery at destination. Containers and closures shall comply with the Surface Transportation Board, Uniform Freight Classification Rules, or regulations of other carriers as applicable to the mode of transportation.

(b) On the front of the package, the Contractor shall clearly identify the contract number under which the product is being provided.

(c) Additional packaging and/or marking requirements are as follows: All mailed information shall be sent to COR at:

NRC Storage & Distribution Facility
ATTN: [redacted]
4934 Boiling Brook Parkway
Rockville, MD 20852

(End of Clause)

D.2 BRANDING

The Contractor is required to use the statement below in any publications, presentations, articles, products, or materials funded under this contract/order, to the extent practical, in order to provide NRC with recognition for its involvement in and contribution to the project. If the work performed is funded entirely with NRC funds, then the contractor must acknowledge that information in its documentation/presentation.

Work Supported by the U.S. Nuclear Regulatory Commission (NRC), Office of the Chief Information Officer, under Contract/order number 31310020C0015.

(End of Clause)

SECTION E - Inspection and Acceptance

E.1 INSPECTION AND ACCEPTANCE BY THE NRC (SEP 2013)

Inspection and acceptance of the deliverable items to be furnished hereunder shall be made by the NRC Contracting Officer's Representative (COR) at the destination, accordance with FAR 52.247-34 - F.o.b. Destination.

Contract Deliverables: See Section B.3 Price/Cost Schedule

(End of Clause)

SECTION F - Deliveries or Performance

F.1 PERIOD OF PERFORMANCE ALTERNATE

This contract shall commence on September 1, 2020 and will expire on August 31, 2021. The term of this contract may be extended at the option of the Government for an additional four (4) years, from September 1, 2021 to August 31, 2025.

Base Period: September 1, 2020 to August 31, 2021

Option Periods:

Option Period 1: September 1, 2021 to August 31, 2022
Option Period 2: September 1, 2022 to August 31, 2023
Option Period 3: September 1, 2023 to August 31, 2024
Option Period 4: September 1, 2024 to August 31, 2025

(End of Clause)

F.2 RECOGNIZED HOLIDAYS

The contractor is not required to perform services on Federal Holidays.

New Year’s Day

Martin Luther King Jr.’s Birthday

President’s Day

Memorial Day

Independence Day

Labor Day

Columbus Day

Veteran’s Day

Thanksgiving Day

Christmas Day

SECTION G - Contract Administration Data

G.1 REGISTRATION IN FEDCONNECT® (JULY 2014)

The Nuclear Regulatory Commission (NRC) uses Compusearch Software Systems' secure and auditable two-way web portal, FedConnect®, to communicate with vendors and contractors. FedConnect® provides bi-directional communication between the vendor/contractor and the NRC throughout pre-award, award, and post-award acquisition phases. Therefore, in order to do business with the NRC, vendors and contractors must register to use FedConnect® at https://www.fedconnect.net/FedConnect. The individual registering in FedConnect® must have authority to bind the vendor/contractor. There is no charge for using FedConnect®. Assistance with FedConnect® is provided by Compusearch Software Systems, not the NRC. FedConnect® contact and assistance information is provided on the FedConnect® web site at https://www.fedconnect.net/FedConnect.

G.2 ELECTRONIC PAYMENT (DEC 2017)

The Debt Collection Improvement Act of 1996 requires that all payments except IRS tax refunds be made by Electronic Funds Transfer. Payment shall be made in accordance with FAR 52.232-33, entitled "Payment by Electronic Funds Transfer-System for Award Management."

To receive payment, the contractor shall prepare invoices in accordance with NRC's Billing Instructions. Claims shall be submitted through the Invoice Processing Platform (IPP) (https://www.ipp.gov/). Back up documentation shall be included as required by the NRC's Billing Instructions.

(End of Clause)

G.3 KEY PERSONNEL. (JAN 1993)

(a) The following individuals are considered to be essential to the successful performance of the work hereunder:

[redacted] - Project Manager

*The contractor agrees that personnel may not be removed from the contract work or replaced without compliance with paragraphs (b) and (c) of this section.

(b) 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 or initially anticipated, the contractor shall immediately notify the contracting officer and shall, subject to the concurrence of the contracting officer, promptly replace the personnel with personnel of at least substantially equal ability and qualifications.

(c) Each request for approval of substitutions must be in writing and contain a detailed explanation of the circumstances necessitating the proposed substitutions. The request must also contain a complete resume for the proposed substitute and other information requested or needed by the contracting officer to evaluate the proposed substitution.

The contracting officer and the project officer shall evaluate the contractor's request and the contracting officer shall promptly notify the contractor of his or her decision in writing.

(d) If the contracting officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated, or have otherwise become unavailable for the contract work is not reasonably forthcoming, or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the contract or the service order, the contract may be terminated by the contracting officer for default or for the convenience of the Government, as appropriate. If the contracting officer finds the contractor at fault for the condition, the contract price or fixed fee may be equitably adjusted downward to compensate the Government for any resultant delay, loss, or damage.

SECTION H - Special Contract Requirements

H.1 INFORMATION TECHNOLOGY (IT) SECURITY REQUIREMENTS – GENERAL (JUL 2016)

Basic Contract IT Security Requirements

The contractor agrees to insert terms that conform substantially to the language of the IT security requirements, excluding any reference to the Changes clause of this contract, into all subcontracts under this contract.

For unclassified information used for the effort, the contractor shall provide an information security categorization document indicating the sensitivity of the information processed as part of this contract if the information security categorization was not provided in the statement of work. The determination shall be made using National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 and must be approved by the Office of the Chief Information Officer (OCIO). The NRC contracting officer (CO) and Contracting Officer's Representative (COR) shall be notified immediately before the contractor begins to process information at a higher sensitivity level.

If the effort includes use or processing of classified information, the NRC CO and COR shall be notified before the contractor begins to process information at a more restrictive classification level.

All work under this contract shall comply with the latest version of policy, procedures and standards. Individual task orders will reference latest versions of standards or exceptions as necessary. These policy, procedures and standards include: NRC Management Directive (MD) volume 12, Security; Computer Security Office policies, procedures and standards; National Institute of Standards and Technology (NIST) guidance and Federal Information Processing Standards (FIPS); and Committee on National Security Systems (CNSS) policy, directives, instructions, and guidance. This information is available at the following links:

NRC Policies, Procedures and Standards (OCIO/ISD – Director, Information Security Directorate, internal website):

http://www.internal.nrc.gov/CSO/policies.html

All NRC Management Directives (public website):

http://www.nrc.gov/reading-rm/doc-collections/management-directives/

NIST SP and FIPS documentation is located at:

http://csrc.nist.gov/

CNSS documents are located at:

http://www.cnss.gov/

When e-mail is used, the contractors shall only use NRC provided e-mail accounts to send and receive sensitive information (information that is not releasable to the public) or mechanisms to protect the information during transmission to NRC that have been approved by OCIO/ISD.

All contractor employees must sign the NRC Agency-Wide Rules of Behavior for Authorized Computer Use prior to being granted access to NRC computing resources.

The contractor shall adhere to following NRC policies, including but not limited to:

Must meet all federally mandated and NRC defined cybersecurity requirements.

• Management Directive 12.5, NRC Cybersecurity Program

• Computer Security Policy for Encryption of Sensitive Data When Outside of Agency Facilities

• Policy for Copying, Scanning, Printing, and Faxing SGI & Classified Information

• Computer Security Information Protection Policy

• Remote Access Policy

• Laptop Security Policy

• Computer Security Incident Response Policy

Contractor will adhere to NRC’s use of personal devices to process and store NRC sensitive information. The NRC’s BYOD program allows NRC employees and contractors to conduct official government business using supported personal smart phones and tablets.

All work performed at non-NRC facilities shall be in facilities, networks, and computers that have been accredited by NRC for processing information at the sensitivity level of the information being processed.

Contract Performance and Closeout

The contractor shall ensure that the NRC data processed during the performance of this contract shall be purged from all data storage components of the contractor’s computer facility, and the contractor will retain no NRC data within 30 calendar days after contract is completed. Until all data is purged, the contractor shall ensure that any NRC data remaining in any storage component will be protected to prevent unauthorized disclosure.

When a contractor employee no longer requires access to an NRC system, the contractor shall notify the COR within 24 hours.

Upon contract completion, the contractor shall provide a status list of all contractor employees who were users of NRC systems and shall note if any users still require access to the system to perform work if a follow-on contract or task order has been issued by NRC.

Control of Information and Data

The contractor shall not publish or disclose in any manner, without the CO's written consent, the details of any security controls or countermeasures either designed or developed by the contractor under this contract or otherwise provided by the NRC.

Any IT system used to process NRC sensitive information shall:

• Include a mechanism to require users to uniquely identify themselves to the system before beginning to perform any other actions that the system is expected to provide.

• Be able to authenticate data that includes information for verifying the claimed identity of individual users (e.g., passwords).

• Protect authentication data so that it cannot be accessed by any unauthorized user.

• Be able to enforce individual accountability by providing the capability to uniquely identify each individual computer system user.

• Report to appropriate security personnel when attempts are made to guess the authentication data whether inadvertently or deliberately.

Access Controls

Any contractor system being used to process NRC data shall be able to define and enforce access privileges for individual users. The discretionary access controls mechanisms shall be configurable to protect objects (e.g., files, folders) from unauthorized access.

The contractor system being used to process NRC data shall provide only essential capabilities and specifically prohibit and/or restrict the use of functions, ports, protocols, and/or services, as specified in the contract/grant.

The contractors shall only use NRC approved methods to send and receive information considered sensitive or classified. Specifically,

• Classified Information - All NRC Classified data being transmitted over a network shall use NSA approved encryption and adhere to guidance in MD 12.2, NRC Classified Information Security Program; MD 12.5, NRC Cybersecurity Program; and any classified encryption guidance provided by the Committee on National Security Systems. Classified processing shall be only within facilities, computers, and spaces that have been specifically approved for classified processing. All NRC personnel who have been or will be granted an account to access any system or network (to include a stand-alone system or network) on which classified information resides must be an NRC authorized classifier. Contractors must follow the above guidance and procedures when requiring access to or handling classified information. Only designated and authorized classifiers of the contractor may have access to classified information or systems.

• SGI Information – All SGI being transmitted over a network shall adhere to guidance in MD 12.7, NRC Safeguards Information Security Program; and MD 12.5, NRC Cybersecurity Program. SGI processing shall be only within facilities, computers, and

spaces that have been specifically approved for SGI processing. Cryptographic modules provided as part of the system shall be validated under the Cryptographic Module Validation Program to conform to NIST FIPS 140-2 overall level 2 and must be operated in FIPS mode. The contractor shall provide the FIPS 140-2 cryptographic module certificate number and a brief description of the encryption module that includes the encryption algorithm(s) used, the key length, and the vendor of the product.

• All NRC personnel who have been or will be granted an account to access any system or network (to include a stand-alone system or network) on which SGI resides must be an NRC authorized classifier.

The most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks must be enforced by the system through assigned access authorizations.

Separation of duties for contractor systems used to process NRC information must be enforced by the system through assigned access authorizations.

The mechanisms within the contractor system or application that enforces access control and other security features shall be continuously protected against tampering and/or unauthorized changes.

Configuration Standards

All systems used to process NRC sensitive information shall meet NRC configuration standards available at: http://www.internal.nrc.gov/CSO/standards.html.

Information Security Training and Awareness Training

Contractors shall ensure that their employees, consultants, and subcontractors that have significant IT responsibilities (e.g., IT administrators, developers, project leads) receive in-depth IT security training in their area of responsibility. This training is at the employer’s expense.

In compliance with OMB policy, individuals with significant cybersecurity responsibilities (e.g., ISSOs, System Administrators) must complete required role-based training before assuming the role. NRC contractors must ensure that their staff receives the requisite role-based cybersecurity training at the contractor’s expense.

Media Handling

All media used by the contractor to store or process NRC information shall be controlled in accordance with the sensitivity level.

The contractor shall not perform sanitization or destruction of media approved for processing NRC information designated as SGI or Classified. The contractor must provide the media to NRC for destruction.

Vulnerability Management

The Contractor must adhere to NRC patch management processes for all systems used to process NRC information. Patch Management reports will made available to the NRC upon request for following security categorizations and reporting timeframes:

• 5 calendar days after being requested for a high sensitivity system

• 10 calendar days after being requested for a moderate sensitivity system

• 15 calendar days after being requested for a low sensitivity system

For any contractor system used to process NRC information, the contractor must ensure that information loaded into the system is scanned for viruses prior to posting; servers are scanned for malware, including viruses, adware, and spyware, on a regular basis; and virus signatures are updated at the following frequency:

• 1 calendar day for a high sensitivity system

• 3 calendar days for a moderate sensitivity system

• 7 calendar days for a low sensitivity system

For any contractor deliverables or information loaded on external hard drives or other electronic devices, the contractor must ensure that, prior to delivery to the NRC, the device, including software and files, is free of malware, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, browser hijacking software, mobile code, or other malicious code.

(End of Clause)

H.2 ANNUAL AND FINAL CONTRACTOR PERFORMANCE EVALUATIONS

Annual and final evaluations of contractor performance under this contract will be prepared in accordance with FAR Subpart 42.15, "Contractor Performance Information," normally at or near the time the contractor is notified of the NRC's intent to exercise the contract option. If the multi-year contract does not have option years, then an annual evaluation will be prepared before the expiration of the contract. Final evaluations of contractor performance will be prepared at the expiration of the contract during the contract closeout process.

The Contracting Officer will transmit the NRC Contracting Officer’s Representative’s (COR) annual and final contractor performance evaluations to the contractor's Project Manager, unless otherwise instructed by the contractor. The contractor will be permitted thirty days to review the document and submit comments, rebutting statements, or additional information.

Where a contractor concurs with, or takes no exception to an annual performance evaluation, the Contracting Officer will consider such evaluation final and releasable for source selection purposes. Disagreements between the parties regarding a performance evaluation will be referred to an individual one level above the Contracting Officer, whose decision will be final.

The Contracting Officer will send a copy of the completed evaluation report, marked "Source Selection Information", to the contractor's Project Manager for their records as soon as practicable after it has been finalized. The completed evaluation report also will be used as a tool to improve communications between the NRC and the contractor and to improve contract performance.

The completed annual performance evaluation will be used to support future award decisions in accordance with FAR 42.1502 and 42.1503. During the period the information is being used to provide source selection information, the completed annual performance evaluation will be released to only two parties - the Federal government personnel performing the source selection evaluation and the contractor under evaluation if the contractor does not have a copy of the report already.

(End of Clause)

H.3 RULES OF BEHAVIOR FOR AUTHORIZED COMPUTER USE

In accordance with Appendix III, "Security of Federal Automated Information Resources," to Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," NRC has established rules of behavior for individual users who access all IT computing resources maintained and operated by the NRC or on behalf of the NRC. In response to the direction from OMB, NRC has issued the "Agency-wide Rules of Behavior for Authorized Computer Use" policy, hereafter referred to as the rules of behavior. The rules of behavior for authorized computer use will be provided to NRC computer users, including contractor personnel, as part of the annual computer security awareness course.

The rules of behavior apply to all NRC employees, contractors, vendors, and agents (users) who have access to any system operated by the NRC or by a contractor or outside entity on behalf of the NRC. This policy does not apply to licensees. The next revision of Management Directive 12.5, "NRC Automated Information Security Program," will include this policy. The rules of behavior can be viewed at http://www.internal.nrc.gov/CSO/documents/ROB.pdf or use NRC's external Web-based ADAMS at http://wba.nrc.gov:8080/ves/ (Under Advanced Search, type ML082190730 in the Query box).

The rules of behavior are effective immediately upon acknowledgement of them by the person who is informed of the requirements contained in those rules of behavior. All current contractor users are required to review and acknowledge the rules of behavior as part of the annual computer security awareness course completion. All new NRC contractor personnel will be required to acknowledge the rules of behavior within one week of commencing work under this contract and then acknowledge as current users thereafter. The acknowledgement statement can be viewed at http://www.internal.nrc.gov/CSO/documents/ROB_Ack.pdf or use NRC's external Web-based ADAMS at http://wba.nrc.gov:8080/ves/ (Under Advanced Search, type ML082190730 in the Query box).

The NRC Computer Security Office will review and update the rules of behavior annually beginning in FY 2011 by December 31st of each year. Contractors shall ensure that their personnel to which this requirement applies acknowledge the rules of behavior before beginning contract performance and, if the period of performance for the contract lasts

more than one year, annually thereafter. Training on the meaning and purpose of the rules of behavior can be provided for contractors upon written request to the NRC Contracting Officer's Representative (COR).

The contractor shall flow down this clause into all subcontracts and other agreements that relate to performance of this contract/order if such subcontracts/agreements will authorize access to NRC electronic and information technology (EIT) as that term is defined in FAR 2.101.

(End of Clause)

H.4 FOREIGN OWNERSHIP, CONTROL, OR INFLUENCE OVER CONTRACTOR

The National Industrial Security Program Operating Manual (NISPOM) implements the provisions of E.O. 12829, "National Industrial Security Program." A company is considered to be under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or otherwise, to direct or decide matters affecting the management or operations of that company in a manner that may result in unauthorized access to classified information or may adversely affect the performance of classified information contracts. (See NRC Management Directive 12.2 – "NRC Classified Information Security Program")

(a) For purposes of this clause, a foreign interest is defined as any of the following:

(1) A foreign government or foreign government agency;

(2) Any form of business enterprise organized under the laws of any country other than the United States or its possessions;

(3) Any form of business enterprise organized or incorporated under the laws of the U.S., or a State or other jurisdiction within the U.S., which is owned, controlled, or influenced by a foreign government, agency, firm, corporation or person; or

(4) Any person who is not a U.S. citizen.

(b) A U.S. company determined to be under FOCI is not eligible for facility clearance (FCL). If a company already has an FCL, the FCL shall be suspended or revoked unless security measures are taken to remove the possibility of unauthorized access to classified information.

(c) For purposes of this clause, subcontractor means any subcontractor at any tier and the term "contracting officer" shall mean NRC contracting officer. When this clause is included in a subcontract, the term "contractor" shall mean subcontractor and the term "contract" shall mean subcontract.

(d) The contractor shall complete and submit and SF-328, DD-441 and DD-441-1 forms, prior to contract award. The information contained in these forms may be used in making a determination as to whether a contractor is eligible to participate in the National Industrial Security Program and have a facility security clearance.

(e) The contractor shall immediately provide the contracting officer written notice of any changes in the extent and nature of FOCI over the contractor which would affect the answers to the questions presented in SF-328, "Certificate Pertaining to Foreign Interest". Further, notice of changes in ownership or control which are required to be reported to the Securities and Exchange Commission, the Federal Trade Commission, or the Department of Justice shall also be furnished concurrently to the contracting officer.

(f) In those cases where a contractor has changes involving FOCI, the NRC must determine whether the changes will pose an undue risk to the common defense and security. In making this determination, the contracting officer shall consider proposals made by the contractor to avoid or mitigate foreign influences.

(g) The contractor agrees to insert terms that conform substantially to the language of this clause including this paragraph (g) in all subcontracts under this contract that will require access to classified information and shall require such subcontractors to submit completed SF-328, DD-441 and DD-441-1 forms prior to award of a subcontract. Information to be provided by a subcontractor pursuant to this clause may be submitted directly to the contracting officer.

(h) Information submitted by the contractor or any affected subcontractor as required pursuant to this clause shall be treated by NRC to the extent permitted by law, as business or financial information submitted in confidence to be used solely for purposes of evaluating FOCI.

(i) The requirements of this clause are in addition to the requirement that a contractor obtain and retain the security clearances required by the contract. This clause shall not operate as a limitation on NRC's rights, including its rights to terminate this contract.

(j) The contracting officer may terminate this contract for default either if the contractor fails to meet obligations imposed by this clause, e.g., provide the information required by this clause, comply with the contracting officer's instructions about safeguarding classified information, or make this clause applicable to subcontractors, or if, in the contracting officer's judgment, the contractor creates a FOCI situation in order to avoid performance or a termination for default. The contracting officer may terminate this contract for convenience if the contractor becomes subject to FOCI and for reasons other than avoidance of performance of the contract, cannot, or chooses not to, avoid or mitigate the FOCI problem.

(End of Clause)

H.5 REPORTING FOREIGN TRAVEL (MAY 2018)

(a) Unofficial (personal) foreign travel to certain designated countries, as described in paragraph (b) below, must be reported by NRC contractors that have been granted any of the following security clearances:

(1) “Q” clearance with Sensitive Compartmented Information(SCI) access;

(2) “Q” clearance;

(3) “L (H)” clearance; or

(4) “L” clearance.

See NRC Management Directive 12.3, NRC Personnel Security Program, for detailed information on each clearance level.

(b) Unofficial (personal) foreign travel to countries designated as Level 3 (Reconsider Travel) and Level 4 (Do Not Travel), by the Department of State in its travel warning system at https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html must be reported to the Office of Administration, Division of Facilities and Security, Personnel Security Branch (by email to PSBReporting.Resource@nrc.gov), prior to departure or within 5 days of return. Travel to countries designated as Level 1 (Exercise Normal Precautions) and Level 2 (Exercise Increased Precautions) need not be reported.

(c) NRC contractors shall ensure that their employees, subcontractor employees, and consultants who have been granted any of the clearances listed in paragraph (a) above comply with the requirements of this clause. Failure to timely report the required information could result in disciplinary action and/or affect eligibility for a security clearance.

(d) The Contractor shall flow this clause down into all subcontracts and agreements related to this contract under which personnel with one of the security clearances identified in paragraph (a) above are performing.

H.6 SAFETY OF ON-SITE CONTRACTOR PERSONNEL

Ensuring the safety of occupants of Federal buildings is a responsibility shared by the professionals implementing our security and safety programs and the persons being protected. The NRC's Office of Administration (ADM) Division of Facilities and Security (DFS) has coordinated an Occupant Emergency Plan (OEP) for NRC Headquarters buildings with local authorities. The OEP has been approved by the Montgomery County Fire and Rescue Service. It is designed to improve building occupants' chances of survival, minimize damage to property, and promptly account for building occupants when necessary.

The contractor's Project Director shall ensure that all personnel working full time on-site at NRC Headquarters read the NRC's OEP, provided electronically on the NRC Intranet at http://www.internal.nrc.gov/ADM/OEP.pdf. The contractor's Project Director also shall emphasize to each staff member that they are to be familiar with and guided by the OEP, as well as by instructions given by emergency response personnel in situations which pose an immediate health or safety threat to building occupants.

The NRC Contracting Officer’s Representative (COR) shall ensure that the contractor's Project Director has communicated the requirement for on-site contractor staff to follow the guidance in the OEP. The NRC Contracting Officer’s Representative (COR) also will assist in accounting for on-site contract persons in the event of a major emergency (e.g., explosion occurs and casualties or injuries are suspected) during which a full evacuation will be required, including the assembly and accountability of occupants. The NRC DFS will conduct drills periodically to train occupants and assess these procedures.

(End of Clause)

H.7 SECURITY REQUIREMENTS FOR ACCESS TO CLASSIFIED MATTER OR INFORMATION (SEP 2013)

Performance under this contract will require access to classified matter or information (National Security Information or Restricted Data) in accordance with the attached NRC Form 187 (See List of Attachments). Prime Contractor personnel, subcontractors or others performing work under this contract shall require a "Q" security clearance (allows access to Top Secret, Secret, and Confidential National Security Information and Restricted Data) or an "L" security clearance (allows access to Secret and Confidential National Security Information and/or Confidential Restricted Data).

The Contractor must identify all individuals to work under this contract. The NRC sponsoring office shall make the final determination of the type of security clearance required for all individuals working under this contract.

The Contractor shall conduct a preliminary security interview or review for each of its employees, subcontractor employees and consultants, and submit to the Government only the names of candidates that have a reasonable probability of obtaining the level of security clearance for which the candidate has been proposed. The Contractor will pre-screen applicants for the following:

(a) pending criminal charges or proceedings; (b) felony arrest records including alcohol related arrest within the last seven (7) years; (c) record of any military courts-martial charges and proceedings in the last seven (7) years and courts-martial convictions in the last ten (10) years; (d)any involvement in hate crimes; (e) involvement in any group or organization that espouses extra-legal violence as a legitimate means to an end; (f) dual or multiple citizenship including the issuance of a foreign passport in the last seven (7) years; (g) illegal use possession, or distribution of narcotics or other controlled substances within the last seven (7) years; (h) financial issues regarding delinquent debts, liens, garnishments, bankruptcy and civil court actions in the last seven (7) years.

The Contractor will make a written record of their pre-screening interview or review (including any information to mitigate the responses to items listed in (a) - (h)), and have the candidate verify the record, sign and date it. Two (2) copies of the signed interview record or review will be supplied to DFS/PSB with the applicant's completed security application package.

The Contractor will further ensure that all Contractor employees, subcontractor employees and consultants for classified information access approval complete all security applications required by this clause within fourteen (14) calendar days of notification by DFS/PSB of initiation of the application process. Timely receipt of properly completed security applications (submitted for candidates that have a reasonable probability of obtaining the level of security clearance for which the candidate has been proposed) is a contract requirement. Failure of the Contractor to comply with this condition may be a basis to cancel the award, or terminate the contract for default, or offset from the contract's invoiced cost or price the NRC's incurred costs or delays as a result of inadequate pre-screening by the Contractor. In the event of termination or cancellation, the Government may select another firm for contract award.

Such Contractor personnel shall be subject to the NRC Contractor personnel security requirements of NRC Management Directive (MD) 12.3, Part I and 10 CFR Part 10.11, which is hereby incorporated by reference and made a part of this contract as though fully set forth herein, and will require a favorably adjudicated Single Scope Background Investigation (SSBI) for "Q" clearances or a favorably adjudicated Access National Agency Check and Inquiries (ANACI), or higher level investigation depending on the position the individual will occupy, for "L" clearances.

A Contractor employee shall not have access to classified information until he/ she is granted a security clearance by DFS/PSB, based on a favorably adjudicated investigation. In the event the Contractor employee's investigation cannot be favorably adjudicated, any interim access approval could possibly be revoked and the individual could be subsequently removed from performing under the contract. If interim approval access is revoked or denied, the Contractor is responsible for assigning another individual to perform the necessary work under this contract without delay to the contract's performance schedule, or without adverse impact to any other terms or conditions of the contract. The individual will be subject to a reinvestigation every five (5) years for "Q" clearances and every ten (10) years for "L" clearances.

CORs are responsible for submitting the completed access/clearance request package as well as other documentation that is necessary to DFS/PSB. The contractor shall submit a completed security forms packet, including the OPM Standard Form (SF) 86 (online Questionnaire for National Security Positions), two (2) copies of the Contractor's signed pre-screening record and two (2) FD 258 fingerprint charts, to DFS/PSB for review and adjudication, prior to submission to the Office of Personnel Management for investigation. The individual may start working under this contract before a final clearance is granted if a temporary access determination can be made by DFS/PSB after the review of the security package. If the individual is granted a temporary access authorization, the individual may not have access to classified information under this contract until DFS/PSB has granted them the appropriate security clearance, and the Contractor has read, understood, and signed the SF 312, "Classified Information Nondisclosure Agreement." The Contractor shall assure that all forms are accurate, complete, and legible (except for Part 2 of the questionnaire, which is required to be completed in private and submitted by the individual to the Contractor in a sealed envelope), as set forth in NRC MD 12.3. Based on DFS/PSB review of the applicant's investigation, the individual may be denied his/her security clearance in accordance with the due process procedures set forth in MD 12.3, E.O. 12968, and 10 CFR Part 10.11.

In accordance with NRCAR 2052.204-70 cleared Contractors shall be subject to the attached NRC Form 187 (See Section J for List of Attachments), MD 12.3, SF- 86 and Contractor's signed record or review of the pre-screening which furnishes the basis for providing security requirements to prime Contractors, subcontractors or others who have or may have an NRC contractual relationship which requires access to classified information.

CANCELLATION OR TERMINATION OF SECURITY CLEARANCE ACCESS/REQUEST

When a request for clearance investigation is to be withdrawn or canceled, the Contractor shall immediately notify the COR by telephone so that the investigation may

be promptly discontinued. The notification shall contain the full name of the individual, and the date of the request. Telephone notifications must be promptly confirmed in writing by the Contractor to the COR who will forward the confirmation via email to DFS/PSB. Additionally, DFS/PSB must be immediately notified in writing when an individual no longer requires access to Government classified information, including the voluntary or involuntary separation of employment of an individual who has been approved for or is being processed for access under the NRC "Personnel Security Program."

(End of Clause)

H.8 NRC INFORMATION TECHNOLOGY SECURITY TRAINING (MAY 2016)

NRC INFORMATION TECHNOLOGY SECURITY TRAINING (MAY 2016)

NRC contractors shall ensure that their employees, consultants, and subcontractors with access to the agency's information technology (IT) equipment and/or IT services complete NRC's online initial and refresher IT security training requirements to ensure that their knowledge of IT threats, vulnerabilities, and associated countermeasures remains current. Both the initial and refresher IT security training courses generally last an hour or less and can be taken during the employee's regularly scheduled work day.

Contractor employees, consultants, and subcontractors shall complete the NRC's online annual, "Computer Security Awareness" course on the same day that they receive access to the agency's IT equipment and/or services, as their first action using the equipment/service. For those contractor employees, consultants, and subcontractors who are already working under this contract, the on-line training must be completed in accordance with agency Network Announcements issued throughout the year, within three weeks of issuance of this modification.

Additional annual required online NRC training includes but is not limited to the following:

(1) Information Security (INFOSEC) Awareness

(2) Continuity of Operations (COOP) Awareness

(3) Defensive Counterintelligence and Insider Threat Awareness

(4) No FEAR Act

(5) Personally Identifiable Information (PII) and Privacy Act Responsibilities Awareness

Contractor employees, consultants, and subcontractors who have been granted access to NRC information technology equipment and/or IT services must continue to take IT security refresher training offered online by the NRC throughout the term of the contract. Contractor employees will receive notice of NRC's online IT security refresher training requirements through agency-wide notices.

Contractor Monthly Letter Status Reports (MLSR) must include the following information for all completed training:

(1) the name of the individual completing the course;

(2) the course title; and

(3) the course completion date.

The MLSR must also include the following information for those individuals who have not completed their required training:

(1) the name of the individual who has not yet completed the training;

(2) the title of the course(s) which must still be completed; and

(3) the anticipated course completion date(s).

The NRC reserves the right to deny or withdraw Contractor use or access to NRC IT equipment and/or services, and/or take other appropriate contract administrative actions (e.g., disallow costs, terminate for cause) should the Contractor violate the Contractor's responsibility under this clause.

(End of Clause)

H.9 AUTHORITY TO USE GOVERNMENT PROVIDED SPACE AT NRC HEADQUARTERS (SEP 2013)

Prior to occupying any Government provided space at NRC Headquarters in Rockville Maryland, the Contractor shall obtain written authorization to occupy specifically designated government space, via the NRC Contracting Officer’s Representative (COR), from the Chief, Space Design Branch, Office of Administration. Failure to obtain this prior authorization can result in one, or a combination, of the following remedies as deemed appropriate by the Contracting Officer.

(1) Rental charge for the space occupied will be deducted from the invoice amount due the Contractor

(2) Removal from the space occupied

(3) Contract Termination

(End of Clause)

H.10 DRUG FREE WORKPLACE TESTING: UNESCORTED ACCESS TO NUCLEAR FACILITIES, ACCESS TO CLASSIFIED INFORMATION OR SAFEGUARDS INFORMATION, OR PERFORMING IN SPECIALLY SENSITIVE POSITIONS (MARCH 2019)

The following Contractor employees, subcontractor personnel, and consultants proposed for performance or performing under this contract shall be subject to pre-assignment, random, reasonable suspicion, and post-accident drug testing: (1) individuals who have access to classified information (National Security Information and/or Restricted Data); (2) individuals who have access to Safeguards information (section 147 of the Atomic Energy Act of 1954, as amended); (3) individuals who are authorized to carry firearms while performing work under this contract; (4) individuals who are required to operate government vehicles or transport passengers for the NRC; (5) individuals who are

required to operate hazardous equipment at NRC facilities; (6) individuals who administer the agency's drug program or who have Employee Assistance Program duties; (7) individuals who have unescorted access to vital or protected areas of Nuclear Power Plants, Category 1 Fuel Cycle Facilities, or Uranium Enrichment Facilities; or (8) incident/emergency response personnel (including on-call).

H.11 CONTRACTOR RESPONSIBILITY FOR PROTECTING PERSONALLY IDENTIFIABLE INFORMATION (PII)

In accordance with the Office of Management and Budget's guidance to Federal agencies and the Nuclear Regulatory Commission's (NRC) implementing policy and procedures, a contractor (including subcontractors and contractor employees), who performs work on behalf of the NRC, is responsible for protecting, from unauthorized access or disclosure, personally identifiable information (PII) that may be provided, developed, maintained, collected, used, or disseminated, whether in paper, electronic, or other format, during performance of this contract.

A contractor who has access to NRC owned or controlled PII, whether provided to the contractor by the NRC or developed, maintained, collected, used, or disseminated by the contractor during the course of contract performance, must comply with the following requirements:

(1) General. In addition to implementing the specific requirements set forth in this clause, the contractor must adhere to all other applicable NRC guidance, policy and requirements for the handling and protection of NRC owned or controlled PII. The contractor is responsible for making sure that it has an adequate understanding of such guidance, policy and requirements.

(2) Use, Ownership, and Nondisclosure. A contractor may use NRC owned or controlled PII solely for purposes of this contract, and may not collect or use such PII for any purpose outside the contract without the prior written approval of the NRC Contracting Officer. The contractor must restrict access to such information to only those contractor employees who need the information to perform work under this contract, and must ensure that each such contractor employee (including subcontractors' employees) signs a nondisclosure agreement, in a form suitable to the NRC Contracting Officer, prior to being granted access to the information. The NRC retains sole ownership and rights to its PII. Unless the contract states otherwise, upon completion of the contract, the contractor must turn over all PII in its possession to the NRC, and must certify in writing that it has not retained any NRC owned or controlled PII except as otherwise authorized in writing by the NRC Contracting Officer.

(3) Security Plan. When applicable, and unless waived in writing by the NRC Contracting Officer, the contractor must work with the NRC to develop and implement a security plan setting forth adequate procedures for the protection of NRC owned or controlled PII as well as the procedures which the contractor must follow for notifying the NRC in the event of any security breach. The plan will be incorporated into the contract and must be implemented and followed by the contractor once it has been approved by the NRC Contracting Officer. If the contract does not include a security plan at the time of contract award, a plan must be submitted for the approval of the NRC Contracting Officer within 30 days after contract award.

(4) Breach Notification. The contractor must immediately notify the NRC Contracting Officer and the NRC Contracting Officer's Representative (COR) upon discovery of any suspected or confirmed breach in the security of NRC owned or controlled PII.

(5) Legal Demands for Information. If a legal demand is made for NRC owned or controlled PII (such as by subpoena), the contractor must immediately notify the NRC Contracting Officer and the NRC Contracting Officer's Representative (COR). After notification, the NRC will determine whether and to what extent to comply with the legal demand. The Contracting Officer will then notify the contractor in writing of the determination and such notice will indicate the extent of disclosure authorized, if any. The contractor may only release the information specifically demanded with the written permission of the NRC Contracting Officer.

(6) Audits. The NRC may audit the contractor's compliance with the requirements of this clause, including through the use of online compliance software.

(7) Flow-down. The prime contractor will flow this clause down to subcontractors that would be covered by any portion of this clause, as if they were the prime contractor.

(8) Remedies:

(a) The contractor is responsible for implementing and maintaining adequate security controls to prevent the loss of control or unauthorized disclosure of NRC owned or controlled PII in its possession. Furthermore, the contractor is responsible for reporting any known or suspected loss of control or unauthorized access to PII to the NRC in accordance with the provisions set forth in Article 4 above.

(b) Should the contractor fail to meet its responsibilities under this clause, the NRC reserves the right to take appropriate steps to mitigate the contractor's violation of this clause. This may include, at the sole discretion of the NRC, termination of the subject contract.

(9) Indemnification. Notwithstanding any other remedies available to the NRC, the contractor will indemnify the NRC against all liability (including costs and fees) for any damages arising out of violations of this clause.

(End of Clause)

H.12 GREEN PURCHASING (SEP 2015)

(a) In furtherance of the sustainable acquisition goals of Executive Order (EO) 13693, "Planning for Federal Sustainability in the Next Decade," products and services provided under this contract/order shall be energy efficient (EnergyStar® or Federal Energy Management Program - FEMP-designated products), water efficient, biobased, environmentally preferable (excluding EPEAT®-registered products), non-ozone depleting, contain recycled content, or are non- or low toxic alternatives or hazardous constituents (e.g., non-VOC paint), where such products and services meet agency performance requirements. See: Executive Order (EO) 13693, "Planning for Federal Sustainability in the Next Decade."

(b) The NRC and contractor may negotiate during the contract term to permit the substitution or addition of designated recycled content products (i.e., Comprehensive Procurement Guidelines - CPG), EPEAT®-registered products, EnergyStar®- and FEMP designated energy efficient products and appliances, USDA designated biobased products (Biopreferred® program), environmentally preferable products, WaterSense and other water efficient products, products containing non- or lower-ozone depleting substances (i.e., SNAP), and products containing non- or low-toxic or hazardous constituents (e.g., non-VOC paint), when such products and services are readily available at a competitive cost and satisfy the NRC's performance needs.

(c) The contractor shall flow down this clause into all subcontracts and other agreements that relate to performance of this contract/order.

(End of Clause)

H.13 USE OF AUTOMATED CLEARING HOUSE (ACH) ELECTRONIC PAYMENT/REMITTANCE ADDRESS

The Debt Collection Improvement Act of 1996 requires that all Federal payments except IRS tax refunds be made by Electronic Funds Transfer. It is the policy of the Nuclear Regulatory Commission to pay government vendors by the Automated Clearing House (ACH) electronic funds transfer payment system. Item 15C of the Standard Form 33 may be disregarded.

(End of Clause)

H.14 AWARD NOTIFICATION AND COMMITMENT OF PUBLIC FUNDS

(a) All offerors will receive preaward and postaward notices in accordance with FAR 15.503.

(b) It is also brought to your attention that the contracting officer is the only individual who can legally obligate funds or commit the NRC to the expenditure of public funds in connection with this procurement. This means that unless provided in a contract document or specifically authorized by the contracting officer, NRC technical personnel may not issue contract modifications, give formal contractual commitments, or otherwise bind, commit, or obligate the NRC contractually. Informal unauthorized commitments, which do not obligate the NRC and do not entitle the contractor to payment, may include:

(1) Encouraging a potential contractor to incur costs prior to receiving a contract;

(2) Requesting or requiring a contractor to make changes under a contract without formal contract modifications;

(3) Encouraging a contractor to incur costs under a cost-reimbursable contract in excess of those costs contractually allowable; and

(4) Committing the Government to a course of action with regard to a potential contract, contract change, claim, or dispute.

(End of Clause)

SECTION I - Contract Clauses

NRCAR Clauses Incorporated By Reference

2052.204-70 SECURITY. (OCT 1999)

2052.209-72 CONTRACTOR ORGANIZATIONAL CONFLICTS OF INTEREST. (JAN 1993)

2052.215-73 AWARD NOTIFICATION AND COMMITMENT OF PUBLIC FUNDS (OCT 1999)

2052.222-70 NONDISCRIMINATION BECAUSE OF AGE. (JAN 1993)

NRCAR Clauses Incorporated By Full Text

I.1 2052.204-71 SITE ACCESS BADGE REQUIREMENTS. (JAN 1993)

During the life of this contract, the rights of ingress and egress for contractor personnel must be made available as required. In this regard, all contractor personnel whose duties under this contract require their presence on-site shall be clearly identifiable by a distinctive badge furnished by the Government. The Project Officer shall assist the contractor in obtaining the badges for contractor personnel. It is the sole responsibility of the contractor to ensure that each employee has proper identification at all times. All prescribed identification must be immediately delivered to the Security Office for cancellation or disposition upon the termination of employment of any contractor personnel. Contractor personnel shall have this identification in their possession during on-site performance under this contract. It is the contractor's duty to assure that contractor personnel enter only those work areas necessary for performance of contract work and to assure the safeguarding of any Government records or data that contractor personnel may come into contact with.

(End of Clause)

I.2 2052.215-71 PROJECT OFFICER AUTHORITY. (OCT 1999) - ALTERNATE II (OCT 1999)

(a) The contracting officer's authorized representative, hereinafter referred to as the COR, for this contract is:

Name: [redacted]
Email Address: [redacted]
Telephone Number: [redacted]

(b) The COR shall:

(1) Monitor contractor performance and recommend changes in requirements to the contracting officer.

(2) Inspect and accept products/services provided under the contract.

(3) Review all contractor invoices/vouchers requesting payment for products/services provided under the contract and make recommendations for approval, disapproval, or suspension.

(c) The COR may not make changes to the express terms and conditions of this contract.

*To be incorporated into any resultant contract

(End of Clause)

FAR Clauses Incorporated By Reference

52.202-1 DEFINITIONS. (JUN 2020)

52.203-3 GRATUITIES. (APR 1984)

52.203-12 LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS. (JUN 2020)

52.203-16 PREVENTING PERSONAL CONFLICTS OF INTEREST. (JUN 2020)

52.203-17 CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS. (JUN 2020)

52.204-2 SECURITY REQUIREMENTS. (AUG 1996)

52.204-4 PRINTED OR COPIED DOUBLE-SIDED ON POSTCONSUMER FIBER CONTENT PAPER. (MAY 2011)

52.204-9 PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL. (JAN 2011)

52.204-13 SYSTEM FOR AWARD MANAGEMENT MAINTENANCE. (OCT 2018)

52.204-19 INCORPORATION BY REFERENCE OF REPRESENTATIONS AND CERTIFICATIONS. (DEC 2014)

52.215-23 LIMITATIONS ON PASS-THROUGH CHARGES. (JUN 2020)

52.223-6 DRUG-FREE WORKPLACE. (MAY 2001)

52.223-10 WASTE REDUCTION PROGRAM. (MAY 2011)

52.224-1 PRIVACY ACT NOTIFICATION. (APR 1984)

52.224-2 PRIVACY ACT. (APR 1984)

52.224-3 PRIVACY TRAINING. (JAN 2017) - ALTERNATE I (JAN 2017)

52.232-39 UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS. (JUN 2013)

52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS. (DEC 2013)

52.237-2 PROTECTION OF GOVERNMENT BUILDINGS, EQUIPMENT, AND VEGETATION. (APR 1984)

52.242-13 BANKRUPTCY. (JUL 1995)

52.245-1 GOVERNMENT PROPERTY. (JAN 2017)

52.245-9 USE AND CHARGES. (APR 2012)

FAR Clauses Incorporated By Full Text

I.3 52.212-4 CONTRACT TERMS AND CONDITIONS - COMMERCIAL ITEMS. (OCT 2018)

(a) *Inspection/Acceptance*. The Contractor shall only tender for acceptance those items that conform to the requirements of this contract. The Government reserves the right to inspect or test any supplies or services that have been tendered for acceptance. The Government may require repair or replacement of nonconforming supplies or reperformance of nonconforming services at no increase in contract price. If repair/replacement or reperformance will not correct the defects or is not possible, the Government may seek an equitable price reduction or adequate consideration for acceptance of nonconforming supplies or services. The Government must exercise its postacceptance rights (1) within a reasonable time after the defect was discovered or should have been discovered; and (2) before any substantial change occurs in the condition of the item, unless the change is due to the defect in the item.

(b) *Assignment.* The Contractor or its assignee may assign its rights to receive payment due as a result of performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency in accordance with the Assignment of Claims Act (31 U.S.C. 3727). However, when a third party makes payment (e.g., use of the Governmentwide commercial purchase card), the Contractor may not assign its rights to receive payment under this contract.

(c) *Changes*. Changes in the terms and conditions of this contract may be made only by written agreement of the parties.

(d) *Disputes*. This contract is subject to 41 U.S.C. chapter 71, Contract Disputes. Failure of the parties to this contract to reach agreement on any request for equitable adjustment, claim, appeal or action arising under or relating to this contract shall be a dispute to be resolved in accordance with the clause at FAR 52.233-1, Disputes, which is incorporated herein by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.

(e) *Definitions*. The clause at FAR 52.202-1, Definitions, is incorporated herein by reference.

(f) *Excusable delays*. The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.

(g) *Invoice.* (1) The Contractor shall submit an original invoice and three copies (or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include-

(i) Name and address of the Contractor;

(ii) Invoice date and number;

(iii) Contract number, line item number and, if applicable, the order number;

(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;

(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;

(vi) Terms of any discount for prompt payment offered;

(vii) Name and address of official to whom payment is to be sent;

(viii) Name, title, and phone number of person to notify in event of defective invoice; and

(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.

(x) Electronic funds transfer (EFT) banking information.

(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.

(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (e.g., 52.232-33, Payment by

Electronic Funds Transfer-System for Award Management, or 52.232-34, Payment by Electronic Funds Transfer-Other Than System for Award Management), or applicable agency procedures.

(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment regulations at 5 CFR part 1315.

(h) *Patent indemnity*. The Contractor shall indemnify the Government and its officers, employees and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark or copyright, arising out of the performance of this contract, provided the Contractor is reasonably notified of such claims and proceedings.

(i) *Payment*- (1) *Items accepted.* Payment shall be made for items accepted by the Government that have been delivered to the delivery destinations set forth in this contract.

(2) *Prompt payment.* The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR part 1315.

(3) *Electronic Funds Transfer (EFT).* If the Government makes payment by EFT, see 52.212-5(b) for the appropriate EFT clause.

(4) *Discount.* In connection with any discount offered for early payment, time shall be computed from the date of the invoice. For the purpose of computing the discount earned, payment shall be considered to have been made on the date which appears on the payment check or the specified payment date if an electronic funds transfer payment is made.

(5) *Overpayments.* If the Contractor becomes aware of a duplicate contract financing or invoice payment or that the Government has otherwise overpaid on a contract financing or invoice payment, the Contractor shall-

(i) Remit the overpayment amount to the payment office cited in the contract along with a description of the overpayment including the-

(A) Circumstances of the overpayment (*e.g.,* duplicate payment, erroneous payment, liquidation errors, date(s) of overpayment);

(B) Affected contract number and delivery order number, if applicable;

(C) Affected line item or subline item, if applicable; and

(D) Contractor point of contact.

(ii) Provide a copy of the remittance and supporting documentation to the Contracting Officer.

(6) *Interest.* (i) All amounts that become payable by the Contractor to the Government under this contract shall bear simple interest from the date due until paid unless paid within 30 days of becoming due. The interest rate shall be the interest rate established by the Secretary of the Treasury as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, as provided in (i)(6)(v) of this clause, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid.

(ii) The Government may issue a demand for payment to the Contractor upon finding a debt is due under the contract.

(iii) *Final decisions.* The Contracting Officer will issue a final decision as required by 33.211 if-

(A) The Contracting Officer and the Contractor are unable to reach agreement on the existence or amount of a debt within 30 days;

(B) The Contractor fails to liquidate a debt previously demanded by the Contracting Officer within the timeline specified in the demand for payment unless the amounts were not repaid because the Contractor has requested an installment payment agreement; or

(C) The Contractor requests a deferment of collection on a debt previously demanded by the Contracting Officer (see 32.607-2).

(iv) If a demand for payment was previously issued for the debt, the demand for payment included in the final decision shall identify the same due date as the original demand for payment.

(v) Amounts shall be due at the earliest of the following dates:

(A) The date fixed under this contract.

(B) The date of the first written demand for payment, including any demand for payment resulting from a default termination.

(vi) The interest charge shall be computed for the actual number of calendar days involved beginning on the due date and ending on-

(A) The date on which the designated office receives payment from the Contractor;

(B) The date of issuance of a Government check to the Contractor from which an amount otherwise payable has been withheld as a credit against the contract debt; or

(C) The date on which an amount withheld and applied to the contract debt would otherwise have become payable to the Contractor.

(vii) The interest charge made under this clause may be reduced under the procedures prescribed in 32.608-2 of the Federal Acquisition Regulation in effect on the date of this contract.

(j) *Risk of loss*. Unless the contract specifically provides otherwise, risk of loss or damage to the supplies provided under this contract shall remain with the Contractor until, and shall pass to the Government upon:

(1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or

(2) Delivery of the supplies to the Government at the destination specified in the contract, if transportation is f.o.b. destination.

(k) *Taxes*. The contract price includes all applicable Federal, State, and local taxes and duties.

(l) *Termination for the Government's convenience*. The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid a percentage of the contract price reflecting the percentage of the work performed prior to the notice of termination, plus reasonable charges the Contractor can demonstrate to the satisfaction of the Government using its standard record keeping system, have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred which reasonably could have been avoided.

(m) *Termination for cause*. The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance. In the event of termination for cause, the Government shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly

terminated this contract for default, such termination shall be deemed a termination for convenience.

(n) *Title*. Unless specified elsewhere in this contract, title to items furnished under this contract shall pass to the Government upon acceptance, regardless of when or where the Government takes physical possession.

(o) *Warranty*. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.

(p) *Limitation of liability*. Except as otherwise provided by an express warranty, the Contractor will not be liable to the Government for consequential damages resulting from any defect or deficiencies in accepted items.

(q) *Other compliances*. The Contractor shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract.

(r) *Compliance with laws unique to Government contracts.* The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. chapter 37, Contract Work Hours and Safety Standards; 41 U.S.C. chapter 87, Kickbacks; 41 U.S.C. 4712 and 10 U.S.C. 2409 relating to whistleblower protections; 49 U.S.C. 40118, Fly American; and 41 U.S.C. chapter 21 relating to procurement integrity.

(s) *Order of precedence*. Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order: (1) the schedule of supplies/services; (2) The Assignments, Disputes, Payments, Invoice, Other Compliances, Compliance with Laws Unique to Government Contracts, and Unauthorized Obligations paragraphs of this clause; (3) the clause at 52.212-5; (4) addenda to this solicitation or contract, including any license agreements for computer software; (5) solicitation provisions if this is a solicitation; (6) other paragraphs of this clause; (7) the Standard Form 1449; (8) other documents, exhibits, and attachments; and (9) the specification.

(t) Removed and reserved.

(u) *Unauthorized Obligations.* (1) Except as stated in paragraph (u)(2) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(i) Any such clause is unenforceable against the Government.

(ii) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it

appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.

(iii) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(2) Paragraph (u)(1) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(v) *Incorporation by reference*. The Contractor's representations and certifications, including those completed electronically via the System for Award Management (SAM), are incorporated by reference into the contract.

(End of clause)

I.4 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS - COMMERCIAL ITEMS. (JUL 2020)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (JUL 2018) (Section 1634 of Pub. L. 115-91).

(3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (AUG 2019) (Section 889(a)(1)(A) of Pub. L. 115-232).

(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015).

(5) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(6) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77 and 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items: (Contracting Officer check as appropriate.)

[X] (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (JUN 2020), with *Alternate I* (OCT 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

[ ] (2) 52.203-13, Contractor Code of Business Ethics and Conduct (JUN 2020) (41 U.S.C. 3509).

[ ] (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (JUN 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

[X] (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (JUN 2020) (Pub. L. 109-282) (31 U.S.C. 6101 note).

(5) (Reserved)

[ ] (6) 52.204-14, Service Contract Reporting Requirements (OCT 2016) (Pub. L. 111-117, section 743 of Div. C).

[ ] (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (OCT 2016) (Pub. L. 111-117, section 743 of Div. C).

[X] (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (JUN 2020) (31 U.S.C. 6101 note).

[X] (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (OCT 2018) (41 U.S.C. 2313).

[ ] (10) (Reserved)

[ ] (11)(i) 52.219-3, Notice of HUBZone Set-Aside or Sole Source Award (MAR 2020) (15 U.S.C. 657a).

[ ] (ii) Alternate I (MAR 2020) of 52.219-3.

[ ] (12)(i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (MAR 2020) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

[ ] (ii) Alternate I (MAR 2020) of 52.219-4.

[ ] (13) (Reserved)

[ ] (14)(i) 52.219-6, Notice of Total Small Business Set-Aside (MAR 2020) (15 U.S.C. 644).

[ ] (ii) Alternate I (MAR 2020) of 52.219-6.

[ ] (15)(i) 52.219-7, Notice of Partial Small Business Set-Aside (MAR 2020) (15 U.S.C. 644).

[ ] (ii) Alternate I (MAR 2020) of 52.219-7.

[X] (16) 52.219-8, Utilization of Small Business Concerns (OCT 2018) (15 U.S.C. 637(d)(2) and (3)).

[ ] (17)(i) 52.219-9, Small Business Subcontracting Plan (JUN 2020) (15 U.S.C. 637(d)(4)).

[ ] (ii) Alternate I (NOV 2016) of 52.219-9.

[ ] (iii) Alternate II (NOV 2016) of 52.219-9.

[ ] (iv) Alternate III (JUN 2020) of 52.219-9.

[ ] (v) Alternate IV (JUN 2020) of 52.219-9.

[X] (18)(i) 52.219-13, Notice of Set-Aside of Orders (MAR 2020) (15 U.S.C. 644(r)).

[X] (ii) Alternate I (MAR 2020) of 52.219-13.

[ ] (19) 52.219-14, Limitations on Subcontracting (MAR 2020) (15 U.S.C. 637(a)(14)).

[ ] (20) 52.219-16, Liquidated Damages-Subcontracting Plan (JAN 1999) (15 U.S.C. 637(d)(4)(F)(i)).

[X] (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (MAR 2020) (15 U.S.C. 657f).

[ ] (22)(i) 52.219-28, Post-Award Small Business Program Rerepresentation (MAY 2020) (15 U.S.C. 632(a)(2)).

[ ] (ii) Alternate I (MAR 2020) of 52.219-28.

[ ] (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business (EDWOSB) Concerns (MAR 2020) (15 U.S.C. 637(m)).

[ ] (24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (MAR 2020) (15 U.S.C. 637(m)).

[ ] (25) 52.219-32, Orders Issued Directly Under Small Business Reserves (MAR 2020) (15 U.S.C. 644(r)).

[X] (26) 52.219-33, Nonmanufacturer Rule (MAR 2020) (15 U.S.C. 637(a)(17)).

[X] (27) 52.222-3, Convict Labor (JUN 2003) (E.O. 11755).

[X] (28) 52.222-19, Child Labor-Cooperation with Authorities and Remedies (JAN 2020) (E.O. 13126).

[X] (29) 52.222-21, Prohibition of Segregated Facilities (APR 2015).

[ ] (30)(i) 52.222-26, Equal Opportunity (SEP 2016) (E.O. 11246).

[X] (ii) Alternate I (FEB 1999) of 52.222-26.

[ ] (31)(i) 52.222-35, Equal Opportunity for Veterans (JUN 2020) (38 U.S.C. 4212).

[X] (ii) Alternate I (JUL 2014) of 52.222-35.

[ ] (32)(i) 52.222-36, Equal Opportunity for Workers with Disabilities (JUN 2020) (29 U.S.C. 793).

[X] (ii) Alternate I (JUL 2014) of 52.222-36.

[X] (33) 52.222-37, Employment Reports on Veterans (JUN 2020) (38 U.S.C. 4212).

[X] (34) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496).

[ ] (35)(i) 52.222-50, Combating Trafficking in Persons (JAN 2019) (22 U.S.C. chapter 78 and E.O. 13627).

[X] (ii) *Alternate I* (MAR 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

[ ] (36) 52.222-54, Employment Eligibility Verification (OCT 2015). (E. O. 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

[ ] (37)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (MAY 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

[ ] (ii) Alternate I (MAY 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

[ ] (38) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (JUN 2016) (E.O. 13693).

[ ] (39) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (JUN 2016) (E.O. 13693).

[ ] (40)(i) 52.223-13, Acquisition of EPEAT®-Registered Imaging Equipment (JUN 2014) (E.O.s 13423 and 13514).

[ ] (ii) Alternate I (OCT 2015) of 52.223-13.

[ ] (41)(i) 52.223-14, Acquisition of EPEAT®-Registered Televisions (JUN 2014) (E.O.s 13423 and 13514).

(ii) Alternate I (JUN 2014) of 52.223-14.

[ ] (42) 52.223-15, Energy Efficiency in Energy-Consuming Products (MAY 2020) (42 U.S.C. 8259b).

[ ] (43)(i) 52.223-16, Acquisition of EPEAT®-Registered Personal Computer Products (OCT 2015) (E.O.s 13423 and 13514).

[X] (ii) Alternate I (JUN 2014) of 52.223-16.

[ ] (44) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (JUN 2020) (E.O. 13513).

[ ] (45) 52.223-20, Aerosols (JUN 2016) (E.O. 13693).

[ ] (46) 52.223-21, Foams (JUN 2016) (E.O. 13693).

[ ] (47)(i) 52.224-3, Privacy Training (JAN 2017) (5 U.S.C. 552a).

[ ] (ii) Alternate I (JAN 2017) of 52.224-3.

[ ] (48) 52.225-1, Buy American-Supplies (MAY 2014) (41 U.S.C. chapter 83).

[ ] (49)(i) 52.225-3, Buy American-Free Trade Agreements-Israeli Trade Act (MAY 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43.

[ ] (ii) Alternate I (MAY 2014) of 52.225-3.

[ ] (iii) Alternate II (MAY 2014) of 52.225-3.

[ ] (iv) Alternate III (MAY 2014) of 52.225-3.

[X] (50) 52.225-5, Trade Agreements (OCT 2019) (19 U.S.C. 2501, *et seq*., 19 U.S.C. 3301 note).

[ ] (51) 52.225-13, Restrictions on Certain Foreign Purchases (JUN 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

[ ] (52) 52.225-26, Contractors Performing Private Security Functions Outside the United States (OCT 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

[ ] (53) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (NOV 2007) (42 U.S.C. 5150).

[ ] (54) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (NOV 2007) (42 U.S.C. 5150).

[ ] (55) 52.229-12, Tax on Certain Foreign Procurements (JUN 2020).

[ ] (56) 52.232-29, Terms for Financing of Purchases of Commercial Items (FEB 2002) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

[X] (57) 52.232-30, Installment Payments for Commercial Items (JAN 2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

[ ] (58) 52.232-33, Payment by Electronic Funds Transfer-System for Award Management (OCT 2018) (31 U.S.C. 3332).

[ ] (59) 52.232-34, Payment by Electronic Funds Transfer - Other than System for Award Management (JUL 2013) (31 U.S.C. 3332).

[ ] (60) 52.232-36, Payment by Third Party (MAY 2014) (31 U.S.C. 3332).

[ ] (61) 52.239-1, Privacy or Security Safeguards (AUG 1996) (5 U.S.C. 552a).

[ ] (62) 52.242-5, Payments to Small Business Subcontractors (JAN 2017)(15 U.S.C. 637(d)(13)).

[ ] (63)(i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (FEB 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631).

[ ] (ii) Alternate I (APR 2003) of 52.247-64.

[X] (iii) Alternate II (FEB 2006) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items: (Contracting Officer check as appropriate.)

[ ] (1) 52.222-41, Service Contract Labor Standards (AUG 2018) (41 U.S.C. chapter 67).

[X] (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (MAY 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

[ ] (3) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (Multiple Year and Option Contracts) (AUG 2018) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

[ ] (4) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (MAY 2014) (29 U.S.C 206 and 41 U.S.C. chapter 67).

[ ] (5) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (MAY 2014) (41 U.S.C. chapter 67).

[X] (6) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (MAY 2014) (41 U.S.C. chapter 67).

[X] (7) 52.222-55, Minimum Wages Under Executive Order 13658 (DEC 2015).

[ ] (8) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

[ ] (9) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (JUN 2020) (42 U.S.C. 1792).

(d) *Comptroller General Examination of Record*. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, as defined in FAR 2.101, on the date of award of this contract, and does not contain the clause at 52.215-2, Audit and Records - Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating

to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) of this paragraph in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause-

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (JUN 2020) (41 U.S.C. 3509).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (JUL 2018) (Section 1634 of Pub. L. 115-91).

(iv) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (AUG 2019) (Section 889(a)(1)(A) of Pub. L. 115-232).

(v) 52.219-8, Utilization of Small Business Concerns (OCT 2018) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds the applicable threshold specified in FAR 19.702(a) on the date of subcontract award, the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(vi) 52.222-21, Prohibition of Segregated Facilities (APR 2015).

(vii) 52.222-26, Equal Opportunity (SEP 2016) (E.O. 11246).

(viii) 52.222-35, Equal Opportunity for Veterans (JUN 2020) (38 U.S.C. 4212).

(ix) 52.222-36, Equal Opportunity for Workers with Disabilities (JUN 2020) (29 U.S.C. 793).

(x) 52.222-37, Employment Reports on Veterans (JUN 2020) (38 U.S.C. 4212).

(xi) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (DEC 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xii) 52.222-41, Service Contract Labor Standards (AUG 2018) (41 U.S.C. chapter 67).

(xiii) [ ] (A) 52.222-50, Combating Trafficking in Persons (JAN 2019) (22 U.S.C. chapter 78 and E.O. 13627).

[ ] (B) Alternate I (MAR 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

(xiv) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (MAY 2014) (41 U.S.C. chapter 67).

(xv) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (MAY 2014) (41 U.S.C. chapter 67).

(xvi) 52.222-54, Employment Eligibility Verification (OCT 2015) (E. O. 12989).

(xvii) 52.222-55, Minimum Wages Under Executive Order 13658 (DEC 2015).

(xviii) 52.222-62 Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

(xix)(A) 52.224-3, Privacy Training (JAN 2017) (5 U.S.C. 552a).

(B) Alternate I (JAN 2017) of 52.224-3.

(xx) 52.225-26, Contractors Performing Private Security Functions Outside the United States (OCT 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xxi) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (JUN 2020) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxii) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (FEB 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor May include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of clause)

I.5 52.217-7 OPTION FOR INCREASED QUANTITY - SEPARATELY PRICED LINE ITEM. (MAR 1989)

The Government may require the delivery of the numbered line item, identified in the Schedule as an option item, in the quantity and at the price stated in the Schedule. The Contracting Officer may exercise the option by written notice to the Contractor within the contract's period of performance. Delivery of added items shall continue at the same rate that like items are called for under the contract, unless the parties otherwise agree.

(End of clause)

I.6 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT. (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within the contracts period of performance; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least seven (7) days (*60 days unless a different number of days is inserted)* before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 5 years(months)(years).

(End of clause)

I.7 52.219-11 SPECIAL 8(A) CONTRACT CONDITIONS. (JAN 2017)

The Small Business Administration (SBA) agrees to the following:

(a) To furnish the supplies or services set forth in this contract according to the specifications and the terms and conditions hereof by subcontracting with an eligible concern pursuant to the provisions of section 8(a) of the Small Business Act, as amended (15 U.S.C. 637(a)).

(b) That in the event SBA does not award a subcontract for all or a part of the work hereunder, this contract may be terminated either in whole or in part without cost to either party.

(c) Except for novation agreements, delegates to the Nuclear Regulatory Commission the responsibility for administering the subcontract to be awarded hereunder with complete authority to take any action on behalf of the Government under the terms and conditions of the subcontract; provided, however, that the Nuclear Regulatory Commission shall give advance notice to

the SBA before it issues a final notice terminating the right of a subcontractor to proceed with further performance, either in whole or in part, under the subcontract for default or for the convenience of the Government.

(d) That payments to be made under any subcontract awarded under this contract will be made directly to the subcontractor by the Nuclear Regulatory Commission .

(e) That the subcontractor awarded a subcontract hereunder shall have the right of appeal from decisions of the Contracting Officer cognizable under the *Disputes* clause of said subcontract.

(f) To notify the Nuclear Regulatory Commission Contracting Officer immediately upon notification by the subcontractor that the owner or owners upon whom 8(a) eligibility was based plan to relinquish ownership or control of the concern.

(End of clause)

I.8 52.219-12 SPECIAL 8(A) SUBCONTRACT CONDITIONS. (OCT 2019)

(a) The Small Business Administration (SBA) has entered into Contract No. 31310020C0015 with the Nuclear Regulatory Commission to furnish the supplies or services as described therein. A copy of the contract is attached hereto and made a part hereof.

(b) The CODEplus, hereafter referred to as the subcontractor, agrees and acknowledges as follows:

(1) That it will, for and on behalf of the SBA, fulfill and perform all of the requirements of Contract No. 31310020C0015 for the consideration stated therein and that it has read and is familiar with each and every part of the contract.

(2) That the SBA has delegated responsibility, except for novation agreements, for the administration of this subcontract to the Nuclear Regulatory Commission with complete authority to take any action on behalf of the Government under the conditions of this subcontract.

(3) That it will notify the Nuclear Regulatory Commission Contracting Officer in writing immediately upon entering an agreement (either oral or written) to transfer all or part of its stock or other ownership interest to any other party.

(c) Payments, including any progress payments under this subcontract, will be made directly to the subcontractor by the CODEplus.

(End of clause)

I.9 52.219-17 SECTION 8(A) AWARD. (OCT 2019)

(a) By execution of a contract, the Small Business Administration (SBA) agrees to the following:

(1) To furnish the supplies or services set forth in the contract according to the specifications and the terms and conditions by subcontracting with the Offeror who has been determined an eligible concern pursuant to the provisions of section 8(a) of the Small Business Act, as amended (15 U.S.C. 637(a)).

(2) Except for novation agreements, delegates to the Nuclear Regulatory Commission the responsibility for administering the contract with complete authority to take any action on behalf of the Government under the terms and conditions of the contract; provided, however that the contracting agency shall give advance notice to the SBA before it issues a final notice terminating the right of the subcontractor to proceed with further performance, either in whole or in part, under the contract.

(3) That payments to be made under the contract will be made directly to the subcontractor by the contracting activity.

(4) To notify the Nuclear Regulatory Commission Contracting Officer immediately upon notification by the subcontractor that the owner or owners upon whom 8(a) eligibility was based plan to relinquish ownership or control of the concern.

(5) That the subcontractor awarded a subcontract hereunder shall have the right of appeal from decisions of the cognizant Contracting Officer under the "Disputes" clause of the subcontract.

(b) The offeror/subcontractor agrees and acknowledges that it will, for and on behalf of the SBA, fulfill and perform all of the requirements of the contract.

(End of clause)

I.10 52.252-2 CLAUSES INCORPORATED BY REFERENCE. (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): www.acquisition.gov/far, www.acquisition.gov/nrcar

(End of clause)

SECTION J - List of Documents, Exhibits and Other Attachments

Attachment Number	Title	Date
1	Instructions_ IPP Billing Instructions for Fixed Price Contracts	08/11/2020