	COTS Hardware or Software	**Development or Maintenance of Custom Applications**	**Outsourced IT Services or On-site Support**	**Requirements herein are incorporated as part the Statement of Work/ Performance Work Statement:** Public Engagement Kiosk System
1	N/A	☐	☐	**Background Investigations.** The Contractor shall perform in accordance with clause **"Security Requirements: Facility Access and Information Technology**."
2	N/A	☐	☑ ☐ Contractor will have access to **Privacy Act System** of Records - Work under this contract will involve design, development or operation of (access to) system(s) of records containing personal information protected by the Privacy Act (5 U.S.C. Section 552a).	**Non-disclosure Agreement.** Prior to receiving access to USGS computers, contractor employees shall be required to sign nondisclosure or other system security agreements, depending on the systems to be used and level of access granted. Applies whenever any contractor employee has unsupervised access to a USGS system (even if only basic network, internet or email or will develop custom applications) such as: • User Access to USGS IT Systems known to contain sensitive or proprietary data • IT Support services (greater than user access) • Development or Maintenance of Custom Applications • On-site contractor support and management of IT system • Off-site contractor Oversight and Management of IT System • IT Security Services **Privacy Act System**: [*Identify covered system(s) to which the contractor may have access*] Work to be performed: *[Summarize nature of the contractor's use of such records, such as]* • User-level access to system containing protected records • Operation or maintenance of Privacy Act System of records or computers hosting such system • Design or modification of a Privacy Act system of records] The contractor is not required or permitted to respond to requests for Privacy Act data or to make decisions about releases of data under the Act. Contractor shall ensure its employees are instructed to safeguard against improper use or release of such data and advise them that violation of the Act may involve criminal penalties. The contractor will comply with FAR clause 52.224-2, Privacy Act, incorporated herein by reference and with DOI Privacy Act regulations at 43 CFR 2, Subpart D

	COTS Hardware or Software	Development or Maintenance of Custom Applications	Outsourced IT Services or On-site Support	Requirements herein are incorporated as part the Statement of Work/ Performance Work Statement:
3	N/A	☐	☐	**Training.** The Contractor shall perform in accordance with clause "Security Requirements: Facility Access and Information Technology" - Contractor employees must successfully complete DOI's end-user computer security awareness training prior to being granted access to DOI data or being issued a user account. Training must be renewed annually. Additionally, the contract employees must sign a Statement of Responsibility (SOR) that states they have read the appropriate Rules of Behavior and other applicable Information security policies.
4	N/A	☐	☐	**Personnel Changes.** The Contractor shall perform in accordance with clause "Security Requirements: Facility Access and Information Technology" - The contractor must notify the COR immediately when an employee working on a DOI system is reassigned or leaves the contractor's employ. Applies whenever any contractor employee has unsupervised access to a USGS system (even if only basic network, internet or email or will develop custom applications) such as: • User Access to USGS IT Systems known to contain sensitive or proprietary data • IT Support services (greater than user access) • Development or Maintenance of Custom Applications * • On-site contractor support and management of IT system • Off-site contractor Oversight and Management of IT System • IT Security Services * *May not be applicable for off-site performance.
5	N/A	☐	☑	**Contractor Location.** The Contractor shall perform in accordance with clause "Security Requirements: Facility Access and Information Technology." Applies whenever any contractor employee has unsupervised access to a USGS system (even if only basic network, internet or email or will develop custom applications) such as: • User Access to USGS IT Systems known to contain sensitive or proprietary data • IT Support services (greater than user access) • Development or Maintenance of Custom Applications • On-site contractor support and management of IT system • Off-site contractor Oversight and Management of IT System • IT Security Services **No portion of the services to be performed hereunder may be performed outside the United States without the express written permission of the Contracting Officer.**

	COTS Hardware or Software	Development or Maintenance of Custom Applications	Outsourced IT Services or On-site Support	Requirements herein are incorporated as part the Statement of Work/ Performance Work Statement:
				If services are proposed to be performed abroad, the Contractor shall provide an acceptable security plan that addresses mitigation of problems related to communication, control, and protecting the confidentiality, integrity, and availability of IT systems and information. A Security Plan Template is available upon request from the Contracting Officer.
6	N/A	☐	N/A	**Applicable Standards.** The Contractor shall perform in accordance with clause "Security Requirements: Facility Access and Information Technology" - Contractor must follow the DOI System Development Life Cycle (SDLC), NIST SP 800-64 and the DOI SDLC Security Integration Guide.
7	N/A	☐	☐	**Asset Valuation-Security Categorization:** The Contractor shall perform in accordance with clause "Security Requirements: Facility Access and Information Technology." ☐ User Access to USGS IT Systems – The Government is responsible for security categorization on USGS systems to which the Contractor may have access under this contract. ☐ IT Support Services greater than User-Level Services Choose one: ➔ ☐ The Government is responsible for security categorization on USGS systems to which the Contractor may have access under this contract. ➔ ☐ The Government has defined the [insert name of system to be developed, operated or maintained by the contractor] to be a [Major Application], [Minor Application] or [General support system] as defined in OMB Circular A-130, Appendix III and NIST SP800-53. The following risk and sensitivity levels have been assigned based on the FIPS 199 and the NIST SP 800-60. Mission impact: Data sensitivity: Risk level: Bureau/departmental/national criticality: ☐ Off-Site Oversight and Management of IT System- The Contractor shall use the FIPS 199 and the NIST SP 800- 60 to determine information types and security categorization based on mission impact, data sensitivity, risk level, and bureau / departmental / national criticality for Contractor-owned and operated systems used to provide services under this contract. Solicitations must include either the complete publication or a reference to public facilities, such as a website or office, where it may be accessed. ☐ IT Security Services - Applies only if the purpose of the contract includes obtaining asset valuation services. The Contractor shall use the FIPS 199 and the NIST SP 800- 60 to determine information types and security categorization based on mission impact, data sensitivity, risk level, and bureau / departmental / national criticality for Contractor-owned and operated systems used to provide services under this contract. Solicitations must include either the complete publication or a reference to public facilities, such as a website or office, where it may be accessed.

	COTS Hardware or Software	Development or Maintenance of Custom Applications	Outsourced IT Services or On-site Support	Requirements herein are incorporated as part the Statement of Work/ Performance Work Statement:
8	☐	☐ The Government shall be granted unlimited rights in software or data produced hereunder as described in **FAR clause 52.227-17**, Rights in Data—Special Works, incorporated by reference herein.	☐ Select either COTS or custom software language as applicable. If both apply, identify software/data deliverables governed by each clause.	**Property Rights.** 1. For Federal Supply Schedule orders or orders under an existing contract, rights to software acquired hereunder are set forth in the basic contract. 2. For open market contracts, the Government's rights in software delivered hereunder shall be as described in software developer's commercial software license agreement or the clause FAR **52.227-19, Commercial Computer Software-Restricted Rights**, whichever is greater.
9	N/A	☐	☐	**Independent Verification and Validation (IV&V).** The Government is responsible for independent software verification and validation prior to being moved into production. ☐ On-Site Contractor Support and Management of IT System Choose one: ➔ ☐ Software will be independently verified and validated by the Government or another selected contractor prior to being moved into production. ➔ ☐ Contractor will ensure that independent verification and validation is performed on software deployed on contractor managed systems containing USGS data, in accordance with DOI SDLC Security Integration Guide ☐ Off-Site Contractor Operation and Management of IT System-Contractor will ensure that independent verification and validation is performed on software deployed on contractor managed systems containing USGS data, in accordance with DOI SDLC Security Integration Guide ☐ IT Security Service - Applies only if the purpose of the contract includes obtaining IV&V services.

	COTS Hardware or Software	Development or Maintenance of Custom Applications	Outsourced IT Services or On-site Support	Requirements herein are incorporated as part the Statement of Work/ Performance Work Statement:
10	N/A	☐ Applies if the purpose of the contract includes obtaining C&A services.	☐	**Certification & Accreditation.** ☐ User Access to USGS IT Systems or IT Supports Services (Greater than User Access Certification and Accreditation on USGS systems to which the Contractor may have access under this contract will be conducted by the Government or another of its contractors. ☐ Development or Maintenance of Custom Applications The contractor will perform Certification and Accreditation (C&A) services on the application developed or maintained hereunder prior to going into production. The application must be re-accredited every three years or whenever there is a major change that affects security. C&A documents will be provided to the COR in both hard copy and electronic forms. The contractor must follow NIST SP 800-37, 800-18, 800-30, 800-60, 800-53A, Federal Information Processing Standard (FIPS) 199 and 200, the associated DOI guides/templates, the DOI Security Test & Evaluation (ST&E) Guide, and the DOI Privacy Impact Assessment. NIST documents are available on the internet at http://csrc.nist.gov/publications/nistpubs/ FIPS documents are available on the internet at http://csrc.nist.gov/publications/nistpubs/. The contractor may request copies of DOI documents by contacting the Contracting Officer. The government reserves the right to conduct the ST&E using either Government personnel or an independent contractor. The contractor will take immediate and timely action to correct or mitigate any weaknesses discovered as necessary to bring the application or system into compliance with the above requirement. ☐ On-Site Contractor Support and Management of IT System or Off-Site Contractor Operation and Management of IT System The Contractor must maintain systems that are compliant with NIST SP 800-18, 800-30, 800-37, 800-53A, 800-60, Federal Information Processing Standard (FIPS) 199 and 200, the associated DOI guides/templates, the DOI Security Test & Evaluation (ST&E) Guide, and the DOI Privacy Impact Assessment. As required by the above, Major Applications and General Support Systems shall be certified and accredited (C&A) prior to going into production and re-accredited every three years or whenever there is a major change that affects security. C&A documents will be provided to the COR in both hard copy and electronic forms. NIST documents are available on the internet at http://csrc.nist.gov/publications/nistpubs/. The contractor may request copies of DOI documents by contacting the Contracting Officer. The government will reserve the right to conduct the ST&E, using either Government personnel or an independent contractor. The contractor will take immediate and timely action to correct or mitigate any weaknesses discovered as necessary to bring the application or system into compliance with the above requirement.
11	N/A for COTS HW & SW, User Access to USGS IT Systems (other than IT services), IT Support Services (User Level or greater access)	N/A	☐	**Internet Logon Banner.** The Contractor shall perform in accordance with clause "Security Requirements: Facility Access and Information Technology." ☐ Development or Maintenance of Custom Applications OR On-Site Contractor Support and Management of IT System OR Off-site Contractor Oversight and Management of IT System- Web-based applications developed or maintained under this contract must contain a USGS approved logon banner: https://portal.doi.net/CIO/ITPMgmt/Documents/IT Standards/IT Security/DOI Security Control Standards (based on NIST SP 800-53 Revision 3)/Access Control v1.4.pdf
12	N/A	☐	✔	**Incident Reporting.** The Contractor shall perform in accordance with contract clause "Security Requirements: Facility Access and Information Technology" - The contractor must report computer security incidents affecting DOI data or systems in accordance with the DOI Computer Incident Response Guide.

	COTS Hardware or Software	Development or Maintenance of Custom Applications	Outsourced IT Services or On-site Support	Requirements herein are incorporated as part the Statement of Work/ Performance Work Statement:
13	☐	☐	☐	**Quality Control.** All software or hardware purchased must be free of malicious code such as viruses, Trojan horse programs, worms, spyware, etc. Validation of this must be written into the contract.
14	N/A	N/A	☐	**Self-Assessment.** The Contractor shall perform in accordance with contract clause "Security Requirements: Facility Access and Information Technology" - The contractor must conduct an annual self-assessment in accordance with annual DOI guidance on all information systems in production.
15	N/A	☐	☐	**Vulnerability Analysis.** Vulnerability Analysis on USGS systems to which the Contractor may have access under this contract will be conducted by the Government or another of its contractors.
16	N/A	☐	☐	**Logon Banner.** Contractor employees who access DOI information systems must acknowledge a government-approved legal warning banner prior to logging on to the system. This includes contractor owned information systems hosting DOI data.
17	N/A	☐	☐	**Security Controls.** The Contractor shall perform in accordance with contract clause "Security Requirements: Facility Access and Information Technology" – The Contractor shall ensure compliance with the security control requirements of the current version of NIST SP 800-53, Rev.1, which are applicable to the security categorization of the data or system. FIPS 199 and the NIST SP 800-60 will be used to determine information types and security categorizations.
18	N/A	N/A	☐	**Contingency Plan.** The Contractor shall perform in accordance with contract clause "Security Requirements: Facility Access and Information Technology." For IT Support Services: The Contractor shall submit a contingency plan in accordance with NIST SP 800-34 and DOI IT Systems Contingency Plan Guide.