IT Security Management Plan	
Firm Name:	Contract No.:
Firm POC and Title:	Contract Performance Period:

This plan describes the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this NASA SBIR/STTR contract _____accordance with NASA FAR Supplement clause 1852.204-76 (Security requirements for unclassified information technology resources).

This contract only requires remote access to one NASA IT system, the SBIR/STTR Proposal Submission Award Management System (ProSAMS) at https://my.prosams.nasa.gov/login-legal-notices. (System Security Plan: ST-9999-M-CIO-5256), for the electronic submission of contract deliverables, including invoices and technical reports. Access to this system is managed through the NASA Account Management System (NAMS) that requires obtaining a NASA Agency User ID and profile password through the Identity and Access Management System (IdMAX). This process is initiated upon self-registration in the SBIR/STTR Awardee Firm ProSAMS. Registration in the SBIR/STTR Awardee Firm ProSAMS shall be limited to those persons involved in the contract negotiation and administration processes. All registered personnel will be required to take NASA Online Annual IT Security Training. Note: This is an annual training requirement for the duration of the contract.

The NASA IT system access _____ shall protect the confidentiality, integrity, and availability of NASA Electronic Information and IT resources and protect NASA Electronic Information from unauthorized disclosure.

As a NASA contractor that processes, manages, transmits, accesses, or stores unclassified electronic information, to include Controlled Unclassified Information (CUI), for NASA in support of NASA's missions, programs, projects and/or institutional requirements, personnel shall understand and adhere to the NIST and NASA IT Security requirements, regulations, policies, and guidelines posted at https://www.nasa.gov/cybersecurity-policies.

CUI information is defined broadly as unclassified information that does not surpass the thresholds for National Security Classifications but is pertinent to the national interest of the United States. As such, the Federal government and/or NASA, pursuant to law or policy, require such information to be protected from disclosure, have special handling safeguards, and have prescribed limits on its exchange or dissemination. When you submit documents to us, we label your information and protect it as CUI.

Access to any additional NASA IT systems and/or Agency data required during the performance of this contract is disclosed below:

_____

_____

_____

_____

1851852.237-72 Access to Sensitive Information

The Computer Security Act of 1987, PL 100-235, defines "sensitive information" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national

interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy."

To assist NASA in accomplishing management activities and administrative functions, _____ shall provide the services as specified in the above referenced contract. If performing this contract entails access to sensitive information, as defined above, _____ agrees to:

1. Utilize any sensitive information coming into its possession only for the purposes of performing the services specified in this contract, and not to improve its own competitive position in another procurement.
2. Safeguard sensitive information coming into its possession from unauthorized use and disclosure.
3. Allow access to sensitive information only to those employees that need it to perform services under this contract.
4. Preclude access and disclosure of sensitive information to persons and entities outside of the Contractor's organization.
5. Train employees who may require access to sensitive information about their obligations to utilize it only to perform the services specified in this contract and to safeguard it from unauthorized use and disclosure.
6. Obtain a written affirmation from each employee that he/she has received and will comply with training on the authorized uses and mandatory protections of sensitive information needed in performing this contract.
7. Administer a monitoring process to ensure that employees comply with all reasonable security procedures, report any breaches to the Contracting Officer, and implement any necessary corrective actions.

_____ recognizes that unauthorized uses or disclosures of sensitive information may result in termination of the contract for default, or in debarment of the Contractor for serious misconduct affecting present responsibility as a government contractor.

NASA Cybersecurity and Privacy Rules of Behavior

All personnel supporting this project will comply with following NASA's Cybersecurity and Privacy Rules of Behavior that outline the user's responsibilities and expected behavior for accessing and using NASA's information systems and data, while ensuring security and compliance with NASA policies. Personnel supporting are responsible for reading and complying with these rules. The full text can be found at https://id.nasa.gov/doc/ITROB.docx.

Incident Response

If an intentional or inadvertent information security incident occurs affecting the confidentiality, integrity, and availability of information, the firm will immediately notify the NASA Security Operations Center (SOC) [1-877-NASA-SEC (877-627-2732) or via the SOC email address (soc@nasa.gov)], or other appropriate NASA officials, including the CO and COR assigned to the contract.

If any NASA IT system or data, including contract deliverables, is compromised, misused, distorted, lost, or destroyed, the firm will immediately notify the NASA Security Operations Center or other appropriate NASA officials, including the CO and COR assigned to the contract.

Additional IT Security Management Procedures

Include any additional Security Management Procedures and Controls. Indicate whether your firm has a NASA approved an IT Security Plan, Risk Assessment, and FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, Assessment in place.

By signing below, _____ acknowledges and understands that unauthorized attempts to upload or change information on NASA servers are strictly prohibited and may be punishable by law, including under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act of 1996. Compliance with applicable laws, policies and standards will be enforced through sanctions commensurate with the level of infraction.

Signature of Firm POC:	Date:

ATTACHMENT 4

Applicable Document List (ADL)

Contractors interested in doing business with NASA and/or providing IT services or solutions to NASA should use this list as a reference for information security requirements.

Document, Subject

- NPR 1382.1B, NASA Privacy Procedural Requirements
- NPD 1382.17J, NASA Privacy Policy
- NPD 1440.6I, NASA Records Management
- NPR 1441.1E, NASA Records Management Program Requirements
- NPD 2540.1K, Acceptable Use of Government Furnished Information Technology Equipment, Services and Resources
- NPD 2800.1F, Managing Information Technology
- NPR 2800.2A, Information and Communication Technology Accessibility
- NPR 2810.1F, Security of Information and Information Systems
- NPD 2810.1F, NASA Information Security Policy
- NPR 2830.1A, NASA Enterprise Architecture Procedures
- NPD 2830.1D, NASA Enterprise Architecture
- NPR 2841.1, Identity, Credential, and Access Management

NASA handbooks related to privacy, cybersecurity and information security are available via the NASA Online Directives Information System (NODIS) at https://nodis3.gsfc.nasa.gov.