TYAD Security Requirements

All TYAD contracts and other acquisition-related documents must ensure privacy and security controls follow the information, and that contractors and service providers protect Privacy Act information in the same way the organization adhering to the Federal Acquisition Regulations (FAR) Privacy Act provisions (Subparts 24.1 and 24.2) and include the specified contract clauses (Parts 52.224-1 and 52.224-2), as appropriate, to ensure that personal information is protected as mandated.

In addition to the changes authorized by the clause of this contract; should Force Protection Condition (FPCON) at the installation change, the Government may require changes in contractor security matters and/or processes.

FPCON impact on work levels. *(Please annotate with an X which may apply)*:

_____ During FPCONs Charlie and Delta, [XXX] services are discontinued. [XXX] services will resume when the FPCON level is reduced to level Bravo or lower.

_____This contract and its employees are considered mission essential. Therefore, all contractor employees are required to report for duty and remain on duty during declared emergencies and/or elevated FPCON levels unless otherwise directed by the contacting officer via the appropriate COR.

(*If Required*) The contractor shall provide support during contingencies, exercises, heightened operations, and adverse weather or security closures in the accomplishment of performance requirements. From time to time, the Base Commander may decide to close all or part of a base in response to an unforeseen emergency or similar occurrence. Such emergencies include adverse weather such as snow, or ice, "an act of God such as tornado or earthquake, or a base disaster such as a gas leak or fire.

Base closure announcements will normally be disseminated by local television and radio station.

Contingency Operations Plan

The Contractor shall prepare and submit a Contingency Operations Plan to the Government. The Contingency Operations Plan shall document Contractor plans and procedures to maintain support during an emergency. The Contingency Operations Plan shall include the following:

- A description of the Contractor's emergency management procedures and policy
- A description of how the Contractor will account for their employees during an emergency
- Planned temporary work locations or alternate facilities
- How the Contractor will communicate with Government during emergencies
- A list of primary and alternate Contractor POCs, each with primary and alternate telephone numbers
- Procedures for protecting Government Furnished Equipment (GFE)/Government furnished property (if any)

- Procedures for safeguarding sensitive and/or classified Government information (if applicable)

Unscheduled gate closures by the Security Police may occur at any time causing all personnel entering or exiting a closed installation to experience a delay. This cannot be predicted or prevented. Contractors are not compensated for unexpected closures or delays. Vehicles operated by contractor personnel are subject to search pursuant to applicable regulations. Any moving violation of any applicable motor vehicle regulation may result in the termination of the contractor employee's installation driving privileges.

The contractor's employees shall become familiar with and obey the regulations of the installation; including fire, traffic, safety and security regulations while on the installation. Contractor employees should only enter restricted areas when required to do so and only upon prior approval. All contractor employees shall carry proper identification with them at all times. The contractor shall ensure compliance with all regulations and orders of the installation which may affect performance.

Antiterrorism (AT) Level I Training. All contractor employees, to include subcontractor employees, requiring access to Army installations, facilities, and controlled access areas shall complete AT Level I awareness training prior to contract report date. This training is required for any additional or new contractor employees, who start after that period. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee, to the COR/POC within **10 calendar days** after completion of training by all employees and subcontractor personnel. AT level I awareness training is available at the following website: http://jko.jten.mil/courses/atl1/launch.html for their training. Completion of contractor employee training will be documented on *ELTY form 583*, TYAD On-Post Training Record, or contractor equivalent. As applicable, contractor employees must complete annual AT awareness training as it pertains the length of the contract.

iWATCH Army Training. The contractor and all associated sub-contractors shall brief all employees on the local iWATCH Army Program. This will consist of utilizing the tools and media products on the informational iWATCH Army website to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR/POC. The iWATCH training is available at the following website: https://myarmyonesource.com select Family Programs and Services, in the drop down boxes select: Go To, iWATCH Army –"See Something, Say Something". The contractor shall notify the COR/POC within **10 calendar days** of review of the information on the website for any new employees or subcontractor personnel to assure the *ELTY form 583* or contractor equivalent is properly documented. Completion of contractor employee training will be documented on *ELTY form 583*, TYAD On-Post Training Record or contractor equivalent.

Access and General Protection/Security Policy and Procedures. Contractor and all associated sub-contractors employees shall comply with applicable installation, facility

and area commander installation/facility access and local security policies and procedures (provided by government representative). The contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by TYAD Law Enforcement. Contractor workforce must comply with all personal identity verification requirements as directed by DoD, HQDA, and/or local policy.

Contractor and all associated sub-contractors employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05/AR 190-13), applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by the government representative), or, at OCONUS locations, in accordance with status of forces agreements and other theater regulations.

A background check and approval from Tobyhanna Army Depot (TYAD) Law Enforcement is required for all contractor and subcontractor personnel prior to on-site access at TYAD. All persons seeking entrance to TYAD shall submit to and comply with all security standards and requirements in force at the time such persons are seeking entry. All contractors, regardless of resident status or citizenship, will be subject to vehicle search and intense in-processing by TYAD security personnel prior to being granted access to TYAD. This security screening process may be time consuming and access may be delayed or denied. The contractor shall ensure ELTY Form 648-C is completed for all contractor and subcontractor personnel requiring depot access to include warranty services. The TYAD point of contact (POC) will provide *ELTY Form 648-C, "Request Access to Tobyhanna Army Depo*t" to the contractor/vendor at least **ten days** prior to the expected visit date for completion. The contractor/vendor shall return the completed *ELTY Form 648-C* to the TYAD POC in a timely manner so the same may be submitted to Security for processing no later than **seven days** prior to the visit. All of the required fields on the form shall be complete and accurate by the contractor/vendor for timely processing. This requirement is inclusive of on-site supervisory or managerial personnel and sub-contractor personnel that the Contractor anticipates will be performing work or visiting on-site. This security screening does not relieve the contractor of any responsibilities to conduct thorough pre-employment background checks and drug screening. Contractor workers will not be granted access to the work site until security screening is completed and access is approved. Any contractor personnel on-site who fail screening will not be permitted further access to TYAD. *See "Access and General Protection/Security Policy and Procedures"*.

Submit the completed *ELTY Forms 648-C* form(s) to the COR or POC. Ensure contracts include the provisions that check for the possibility of and prevent undocumented workers for inclusion in contracted work related to Army missions.

TYAD Security Requirements

The company will ensure that its employees entering Army-controlled installations or facilities have obtained access badges and passes in accordance with facility regulations and that these badges and passes are obtained in advance so as not to delay the accomplishment of contracted services.

Common Access Card (CAC) and Information Systems/Network Access by Contractor Workers. *[If applicable.]* Before CAC issuance, the contractor employee requires, at a minimum, a favorably adjudicated National Agency Check with Inquiries (NACI) or an equivalent or higher investigation in accordance with Army Directive 2014-05. The contractor employee will be issued a CAC only if duties involve one of the following: (1) Both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; (2) Remote access, via logon, to a DoD network using DoD-approved remote access procedures; or (3) Physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of 6 months or more. At the discretion of the sponsoring activity, an initial CAC may be issued based on a favorable review of the FBI fingerprint check and a successfully scheduled NACI at the Office of Personnel Management.

Contractors shall be identified with Government issued identification card (e.g., Common Access Card (CAC) or unit specified identification card). When required, contractor personnel shall comply with local security policies to wear their identification card in a standardized manner, clearly visible attached to the torso of the exterior garment above the belt and below the shoulders except when in use (i.e., inserted in a computer CAC reader) or when in controlled areas requiring other credentials as the primary method of identification. To access any Government base and certain facilities, the contractor shall present required identification card upon demand. Upon exit from Government facilities, the contractor shall conceal their credentials (CAC or other credentials) from plain view. The contractor and Contractor Security Manager/Officer shall coordinate with the COR for Government credential issues.

For contractors that do not require CAC, but require access to a DoD facility or installation. Contractor and all associated subcontractor employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (Army Directive 2014-05/AR 190-13); applicable installation, facility and area commander installation and facility access and local security policies and procedures (provided by Government representative); or, at OCONUS locations, in accordance with status-of-forces agreements and other theater regulations.

Collection of Badges: The Contractor shall account for all forms of Government-provided identification issued to the Contractor employees in connection with performance under this contract. The Contractor shall return such identification to the issuing agency at the earliest of any of the following, unless otherwise determined by the Government:

(1) When no longer needed for contract performance.

(2) Upon completion of the Contractor employee's employment.

(3) Upon contract completion or termination.

The Contracting Officer may delay final payment under a contract if the Contractor fails to comply with these requirements. The Contractor shall insert the substance of this clause, including this paragraph, in all subcontracts when the subcontractor's employees are required to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system. It shall be the responsibility of the prime Contractor to return such identification to the issuing agency in accordance with the terms set forth in of this section, unless otherwise approved in writing by the Contracting Officer. The company will return all issued U.S. Government Common Access Cards, installation badges, and/or access passes to the COR when the contract is completed or when a contractor employee no longer requires access to the installation or facility. Contractor personnel will obtain a vehicle pass for access to the military installation and Common Access Cards (CAC) for computer access, if applicable.

Security and privacy requirements for all Department of Defense-Tobyhanna (TYAD) information technology (IT) procurements.

Applicability: The requirements established in this document apply to all employees, contractors, and users authorized to participate in the TYAD IT procurement process. Further, the requirements established herein apply as the entire contract or order (hereafter referred to as a "contract"), or any portion thereof, includes either or both of the following:

a. Access (Physical or Logical) to Government Information: Physical and Logical Access refers to when contractor personnel (and/or any subcontractor) are expected to have (1) routine physical access to an TYAD-controlled facility; (2) logical access to an TYAD-controlled information system; (3) access to government information, whether in an TYAD-controlled information system or in hard copy; or (4) any combination of circumstances (1) through (3) as per OMB M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors.

b. Operate a Federal System Containing Information: A Contractor (and/or any subcontractor) employee will operate a federal system and information technology containing data that supports the TYAD mission. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of "information technology" (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

TYAD Security Requirements

Requirements: Safeguarding Information and Information Systems In accordance with the Federal Information Processing Standards Publication (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, the Contractor (and/or any subcontractor) shall:

a. Protect Government information and information systems in order to ensure:

- Confidentiality, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information.
- Integrity, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity.
- Availability, which means ensuring timely and reliable access to and use of information.

b. Provide security for any Contractor systems, and information contained therein, connected to a TYAD network or operated by the Contractor on behalf of TYAD regardless of location. In addition, if new or unanticipated threats or hazards are discovered by either the agency or contractor, or if existing safeguards have ceased to function, the discoverer shall immediately, within sixty (60) minutes or less, bring the situation to the attention of the other party.

c. Adopt and implement policies, procedures, controls, and standards that are in effect at the time of contract solicitation and required by the TYAD Information Security Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract. Obtain the TYAD Information Security Program security requirements based on the National Institute of Standards and Technology (NIST) “Framework for Improving Critical Infrastructure Cybersecurity.” The framework contains the five (5) core functions to “Identify,” “Protect,” “Detect,” “Respond (to),” and “Recover (from)” any cybersecurity event.

d. Comply with the Privacy Act requirements and with the Federal Information Security Modernization Act (FISMA) and with the OMB memo M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, Contractor Employee Personnel Security Screenings documents, and FAR clauses as applicable and incorporated into this solicitation/contract. Personally Identifiable Information is defined as below.

Per Office of Management and Budget (OMB) Circular A-130, Personally Identifiable Information (PII) is “information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.” Examples of PII include, but are Security and Privacy Requirements for Information Technology Procurements not limited to the following:

social security number, date and place of birth, mother's maiden name, biometric records, etc.

Per TYAD, sensitive PII is PII that if released improperly could result in harm, embarrassment, inconvenience, or unfairness to the individual whose name or identity is linked to the information. Context must be accounted for in order to determine whether PII is sensitive. Some PII is always sensitive, and some is only sensitive when it is used in a particular context. For example, a list of people subscribing to a government newsletter is generally not sensitive PII; a list of people receiving treatment for substance abuse would always be considered sensitive PII.

The list below is not exhaustive. Context must be accounted for in order to determine whether PII is sensitive. The following types of information are always considered sensitive:

- Social Security Numbers (including using just the last 4 digits of the SSN)
- Date of birth
- Mother's maiden name
- Biometric identifiers (e.g., fingerprint, iris scan, voice print)
- Personal financial information, credit card and purchase card account numbers
- Citizenship and immigration status
- Criminal history • Computer access passwords and security questions
- Medical records

a. Mandatory Training for All Contractor Staff - All contractor (and/or any subcontractor) employees assigned to work on this contract shall complete the applicable TYAD Cybersecurity and Privacy Awareness training (provided upon contract award) before performing any work under this contract (this training is available to new contractors, even if they do not have a PIV card). Thereafter, the employees shall complete the TYAD Cybersecurity and Privacy Awareness training at least annually, during the life of this contract. All provided training shall be compliant with TYAD training policies. Contractor Employees Who Require Access to Government Information Systems. All contractor employees with access to a government information system must be registered in the Army Training Certification Tracking System (ATCTS) at commencement of services and must successfully complete the DOD Information Assurance (IA) Awareness prior to access to the information system and then annually thereafter.

b. Training Records - The contractor (and/or any subcontractor) shall maintain training records for all its employees working under this contract in accordance with TYAD policy. A copy of the training records shall be provided to the COR within 30 days after contract award and annually thereafter, or upon request.

Information assurance (IA)/information technology (IT) training. All contractor employees and associated sub-contractor employees must complete the DoD IA awareness training before issuance of network access and annually thereafter. All

contractor employees working IA/IT functions must comply with DoD and Army training requirements in DoDD 8570.01, DoD 8570.01-M and AR 25-2 within six months of employment.

Information assurance (IA)/information technology (IT) certification. Per DoD 8570.01-M , DFARS 252.239.7001 and AR 25-2, the contractor employees supporting IA/IT functions shall be appropriately certified upon contract award. The baseline certification as stipulated in DoD 8570.01-M must be completed upon contract award.

Acceptable Use Policy: *Users who require TYAD Network access are required annually to digitally sign an Acceptable Use Policy. (AUP)* The Acceptable Use Policy is intended to outline expected behavior in regards to the use of Government information technology (IT) resources and to delineate between authorized and unauthorized operating practices. The Acceptable Use Policy also provides an overview of IT system security policies mandated by TYAD. All Government IT resources, including but not limited to, hardware, software, storage media, and computer and network accounts, provided by TYAD are the property of TYAD. They are to be used for business purposes in serving the interests of the Government and TYAD customers in the course of normal operations. Use of Government IT resources for purposes other than those identified within this policy are strictly prohibited and could negate the security of TYAD IT systems. Effective security is a team effort involving the participation and support of everyone who deals with information and/or information systems. It is the responsibility of everyone to know these guidelines, and to conduct their activities accordingly.
The policy represents the commitment of TYAD to ensure that system and information integrity policy is appropriately defined and implemented, in order to protect TYAD systems from intentional or unintentional acts that may negatively impact system security. The policy applies to the use of information, electronic and computing devices, and network resources to conduct TYAD business. All TYAD employees, contractors, and vendors are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with TYAD policies and standards, and local laws and regulation.
This policy applies to employees, contractors, and vendors. This policy applies to all equipment that is owned or leased by TYAD. This policy covers TYAD entire operational environment, including telework locations/sites.

Employees do not have a right, nor should they have any reasonable expectation, of privacy while using any Government IT resources at any time, including accessing the Internet or using e-mail. To the extent that employees wish that their private activities remain private, they should avoid using Government IT resources such as their TYAD-issued computer, the Internet access, or e-mail for such activities. By using Government IT resources, employees give their consent to disclosing the contents of any files or information maintained using this equipment.

Security Clearances. *[If applicable.]* Performance of work will require access to classified information or equipment IAW the DD Form 254, Contract Security Classification Specification, provided as an attachment. Contractor shall comply with FAR 52.204-2, Security Requirements. This clause involves access to information

classified “Confidential,” “Secret,” or “Top Secret” and requires contractors to comply with— (1) The Security Agreement (DD Form 441), including the National Industrial Security Program Operating Manual (DoD 5220.22-M); (2) any revisions to DOD 5220.22-M, notice of which has been furnished to the contractor. If subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.
The Contractor agrees to insert terms that conform substantially to the language of this clause, but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.
Contractor personnel performing IT sensitive duties are subject to investigative and assignment requirements IAW AR 25-2, AR 380-67, DoD 8570.0 and affiliated regulations. Army regulation available at www.apd.army.mil.

Threat Awareness and Reporting Program (TARP). *[If applicable.]* For all contractors with security clearances, per AR 381-12, TARP contractor employees must receive initial and annual TARP training by a CI Agent or other trainer as specified.

Insider Threat Program. The contractor will establish and maintain an insider threat program to gather, integrate, and report relevant and available information indicative of a potential or actual insider threat, consistent with E.O. 13587 and Presidential Memorandum “National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.”

Contracts that Require an OPSEC Standing Operating Procedure/Plan. The contractor shall develop an OPSEC Standing Operating Procedure (SOP)/Plan within 90 calendar days of contract award, to be reviewed and approved by the responsible Government OPSEC officer, per AR 530-1, Operations Security. This SOP/Plan will include the government's critical information, why it needs to be protected, where it is located, who is responsible for it, and how to protect it. In addition, the contractor shall identify an individual who will be an OPSEC Coordinator. The contractor will ensure this individual becomes OPSEC Level II certified per AR 530-1.

Contracts that Require OPSEC Training. Per AR 530-1, Operations Security, new contractor employees must complete Level I OPSEC training within **30 calendar days** of their reporting for duty. All contractor employees must complete annual OPSEC awareness training. The training is available at the following website: http://cdsetrain.dtic.mil/opsec/index.htm The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee, to the COR/POC within **10 calendar days** after completion of training. Completion of contractor employee training will be documented on *ELTY form 583*, TYAD On-Post Training Record or contractor equivalent.

TYAD Security Requirements

a. Contractor personnel shall not discuss government operations in public or over unprotected or unencrypted communications. Official Business, controlled unclassified information may only be transmitted as directed in the SOW/PWS.

b. Contractor personnel shall not discuss government operations in public or over unprotected or unencrypted communications. Official Business, controlled unclassified information may only be transmitted as directed in the SOW/PWS.

c. The Contractor shall not post to company websites, publications, newsletters or other media any images, data or information that reveal sensitive government operations, personnel, equipment, and/or classified or controlled unclassified information. When in doubt, company press releases related to this contract should be coordinated through the Contracting Officer Representative (COR) or Technical Point of Contact, as applicable.

d. Because observation of events, operations, physical changes, etc. may reveal National Security information, specific restrictions are needed to preclude unintentional release of this information to unauthorized parties. (Unauthorized disclosure and transfer of National Security Information is punishable under 18 USC § 793.) Therefore, contractor personnel shall not disclose to unauthorized third parties, post to unofficial sites (including Social Networking sites) any images, data or information, or observed events that reveal sensitive government operations, personnel, equipment, including, but not limited to:

e. Tactics, techniques and procedures, production or work schedules, any visible or concealed modifications, upgrades, additions to vessels, aircraft, or weapons or equipment; increases, change, or decreases in work/deployment frequency or government personnel, vehicle, vessel or aircraft movements; specialized equipment orders, deliveries, shipments, etc., Unauthorized disclosures and attempts to solicit this type of information by unauthorized third parties or others not affiliated with this contract shall be reported to the installation Security Office, contract point of contact, and your company Facility Security Officer and/or the Defense Security Service. Non-Disclosure requirements remain in effect during the duration of this contract and indefinitely thereafter.

f. Government issued badges, identification shall be removed and/or concealed from plain sight when off station and shall not be left in vehicles or unprotected. Badges and passes may not be duplicated or copied or loaned to others. Lost or stolen identification badges, vehicle passes etc. will be immediately reported to the installation Security Office.

g. Practice OPSEC and implement countermeasures to protect CI and other sensitive unclassified information and execution of military operations performed or supported by the contractor in support of the mission. Protection of CI will include the adherence to and execution of countermeasures which the contractor initiates or as provided by TYAD, for CI on or related to the SOW/PWS.

h. It is strongly recommended the contractor mark and protect related internal production schedules, deliverables, inventories and shortages and identified vulnerabilities related to production of government material. Internal company markings

e.g., Business Sensitive, etc., are appropriate for identifying the aforementioned as sensitive information. Specific Government-provided information, drawings etc., will be protected in accordance with guidance in applicable paragraphs of the SOW.

i. All government information must be destroyed at contract termination or returned to the government at the government's discretion.

Information Security (INFOSEC)

Contractor personnel must comply with local security requirements for entry and exit control for personnel and property at the Government leased facility or any Government facility where work is being performed.

Contractor employees will be required to comply with all Government security regulations and requirements. Initial and periodic security training and briefings will be required. Failure to comply with security requirements can cause for removal and the Contractor will not be permitted to provide service on this contract.

The Contractor shall not divulge any information about DoD files, data processing activities or functions, user identifications, passwords, or any other knowledge that may be gained, to anyone who is not authorized to have access to such information. The Contractor shall observe and comply with the security provisions in effect at the Government leased facility or any other Government facilities were work is being performed. Identification shall be worn and displayed as required.

COMSEC/IT Security. All communications with DOD organizations are subject to communications security (COMSEC) review. All telephone communications networks are continually subject to intercept by unfriendly intelligence organizations. DOD has authorized the military departments to conduct COMSEC monitoring and recording of telephone calls originating from, or terminating at, DOD organizations. Therefore, the contractor is advised that any time contractor place or receive a call they are subject to COMSEC procedures. The contractor shall ensure wide and frequent dissemination of the above information to all employees dealing with DOD information. The contractor shall abide by all Government regulations concerning the authorized use of the Government's computer network, including the restriction against using the network to recruit Government personnel or advertise job openings.

Safeguarding Controlled Unclassified Information (CUI)

CUI is defined as "information that laws, regulations, or Government-wide policies require to have safeguarding or dissemination controls, excluding classified information." The contractor (and/or any subcontractor) must comply with Executive Order 13556, Controlled Unclassified Information, (implemented at 32 CFR, part 2002) when handling CUI. 32 CFR 2002.4(aa) as implemented the term "handling" refers to "…any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re- using, and disposing of the information." 81 Fed. Reg. 63323. All

sensitive information that has been identified as CUI by a regulation or statute, handled by this solicitation/contract, shall be:

a. Marked appropriately;
b. Disclosed to authorized personnel on a “Need-To-Know” basis;
c. Protected in accordance with NIST SP 800-53, Rev. 4 Security and Privacy controls for Federal Information Systems and Organizations applicable baseline if handled by a Contractor system operated on behalf of the agency, or NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations if handled by internal Contractor system; and
d. Returned to TYAD control, destroyed when no longer needed, or held until otherwise directed. Destruction of information and/or data shall be accomplished in accordance with NIST SP 800-88, Guidelines for Media Sanitization.

Safeguarding Sensitive Information: For security purposes, information is or may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The contractor (and/or any subcontractor) shall protect all government information that is or may be sensitive in accordance with FISMA by securing it with a FIPS 140-2 validated solution.

Confidentiality, Integrity, Availability, and Nondisclosure of Information: Any information provided to the contractor (and/or any subcontractor) by TYAD or collected by the contractor on behalf of TYAD shall be used only for the purpose of carrying out the provisions of this contract and shall not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The contractor assumes responsibility for protection of the confidentiality, integrity, and availability of Government records and shall ensure that all work performed by its employees and subcontractors shall be under the supervision of the contractor. Each contractor employee or any of its subcontractors at any level to whom any TYAD records may be made available or disclosed shall be notified in writing by the contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein. The confidentiality, integrity, and availability of such information shall be protected in accordance with TYAD policies and instructions. Unauthorized disclosure of information will be subject to the TYAD sanction policies and/or governed by the following laws and regulations:

- 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records);
- 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information); and
- 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).
- 18 U.S.C. 1030 The Computer Fraud and Abuse Act (CFAA)
- 44 U.S.C. 3301 Definition of Records

Government Access for Security Assessment: In addition to the Inspection Clause in the contract, the contractor (and/or any subcontractor) shall afford the Government access to the contractor’s facilities, installations, operations, documentation, information

systems, and personnel used in performance of this contract to the extent required to carry out a program of security assessment (to include vulnerability testing), investigation, and audit to safeguard Security and Privacy Requirements for Information Technology Procurements against threats and hazards to the confidentiality, integrity, and availability of federal data or to the protection of information systems operated on behalf of TYAD, including but are not limited to:

a. At any tier handling or accessing information, consent to and allow the Government, or an independent third party working at the Government's direction, without notice at any time during a weekday during regular business hours contractor local time, to access contractor and subcontractor installations, facilities, infrastructure, data centers, equipment (including but not limited to all servers, computing devices, and portable media), operations, documentation (whether in electronic, paper, or other forms), databases, and personnel which are used in performance of the contract. The purpose of the access is to facilitate performance inspections and reviews, security and compliance audits, and law enforcement investigations. For security audits, the audit may include but not be limited to such items as buffer overflows, open ports, unnecessary services, lack of user input filtering, cross site scripting vulnerabilities, Structured Query Language (SQL) injection vulnerabilities, and any other known vulnerabilities.

b. At any tier handling or accessing protected information, fully cooperate with all audits, inspections, investigations, forensic analysis, or other reviews or requirements needed to carry out requirements presented in applicable law or policy. Beyond providing access, full cooperation also includes, but is not limited to, disclosure to investigators of information sufficient to identify the nature and extent of any criminal or fraudulent activity and the individuals responsible for that activity. It includes timely and complete production of requested data, metadata, information, and records relevant to any inspection, audit, investigation, or review, and making employees of the contractor available for interview by inspectors, auditors, and investigators upon request. Full cooperation also includes allowing the Government to make reproductions or copies of information and equipment, including, if necessary, collecting a machine or system image capture.

c. Cooperate with inspections, audits, investigations, and reviews.

Portable Electronic Devices (PEDs): Non-Government and/or personally owned portable electronic devices (PEDs) are prohibited in all TYAD buildings with the exception of personally owned cell phones, which are authorized for use in spaces up to and including Controlled Access Areas. The Contractor shall ensure the onsite personnel remain compliant with this PED policy. TYAD instruction defines PEDS as the following: any electronic device designed to be easily transported, with the capability to store, record, receive or transmit text, images, video, or audio data in any format via any transmission medium. PEDS include, but are not limited to, pagers, laptops, radios, compact discs and cassette players/recorders. In addition, this includes removable storage media such as flash memory, memory sticks, multimedia cards and secure

digital cards, micro-drive modules, ZIP drives, ZIP disks, recordable CDs, DVDs, MP3 players, iPADs, digital picture frames, electronic book readers, kindle, nook, cameras, external hard disk drives, and floppy diskettes.

PEDs belonging to an external organization shall not be connected to TYAD networks or infrastructure without prior approval from the TYAD Information Assurance and Compliance Branch. Personally, owned hardware or software shall not be connected or introduced to any TYAD hardware, network or information system infrastructure.

National Defense Authorization Act Section 889 Compliance: DoD, GSA, and NASA have issued an interim rule amending the Federal Acquisition Regulation (FAR) to implement section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2019 (Pub. L. 115-232). Section 889(a)(1)(B) prohibits executive agencies from entering into, extending, or renewing a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, on or after August 13, 2020, unless an exception applies or a waiver is granted. See solicitation provision 52.204-24 and clause 52.204-25.

Physical Security: The Contractor shall be responsible for safeguarding all government equipment, information and property provided for Contractor use. At the close of each work period, government facilities, equipment and materials shall be secured.

Key Control. *[If applicable.]* The Contractor shall establish and implement methods of making sure all keys/key cards issued to the Contractor by the Government are not lost or misplaced and are not used by unauthorized persons. ***NOTE:*** All references to keys include key cards. No keys issued to the Contractor by the Government shall be duplicated. The Contractor shall develop procedures covering key control that shall be included in the Quality Control Plan. Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The Contractor shall immediately report any occurrences of lost or duplicate keys/key cards to the KO.

In the event keys, other than master keys, are lost and/or duplicated, the Contractor shall, upon direction of the KO, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the locks or locks shall be deducted from the monthly payment due to the Contractor. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaces by the Government and the total cost deducted from the monthly payment due to the Contractor.

The Contractor shall prohibit the use of Government issued keys/key cards by any persons other than the Contractor's employees. The Contractor shall prohibit the opening of locked areas by Contractor employees to permit entrance of persons other

than Contractor employees engaged in the performance of assigned work in those areas or personnel authorized entrance by the KO.

Lock Combination. *[If applicable.]* The Contractor shall establish and implement methods of ensuring that all lock combinations are not revealed to unauthorized persons. The Contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations. These procedures shall be included in the Contractor's Quality Control Plan.