Information Assurance (IA) Requirements for TSA Government Acquisitions for OSC
1. Purpose
This Transportation Security Administration (TSA) guidebook provides program office personnel guidance for including Information Assurance (IA) requirements for the acquisition of information technology (IT) related services, equipment, supplies, and/or facilities. The IA requirements identified in this guide are used to protect against cyber and physical threats aimed at federal government personnel, US critical infrastructure, property and information. All clauses in Section 2 “Information Assurance Requirements for TSA Government Acquisitions” should be included with all IT acquisitions, excluding Purchase Card acquisitions.

Table 1: Document Change Log

<table>
<thead>
<tr>
<th>Date</th>
<th>Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 6, 2015</td>
<td>Adding OSC Fundamentals</td>
</tr>
<tr>
<td>July 1, 2015</td>
<td>Drafting section P (PIV) and section Q (EOL and EOS) and section R (Supply Chain)</td>
</tr>
<tr>
<td>June 30, 2015</td>
<td>Added Section “O” for passwords.</td>
</tr>
<tr>
<td>March 6, 2015</td>
<td>Amendment to Section L.1 per request of TSA Privacy Office</td>
</tr>
<tr>
<td>November 7, 2014</td>
<td>Simplified instructions to add all requirements to all IT contracts above $3,000.00 (Purchase Card procurements).</td>
</tr>
<tr>
<td>October 24, 2014</td>
<td>Added FedRamp language for Cloud Services per Sharon Jurado; Added new section for clauses by contract type.</td>
</tr>
<tr>
<td>May 5, 2014</td>
<td>FDCC updated to USCGB per Thao Nguyen and approved by Sharon Jurado.</td>
</tr>
<tr>
<td>November 25, 2013</td>
<td>Risk Management Framework changes submitted by Sharon Jurado.</td>
</tr>
</tbody>
</table>
2. Information Assurance Requirements for TSA Government Acquisitions

A. Controls

A.1. The Contractor shall comply with Department of Homeland Security (DHS) and Transportation Security Administration (TSA) technical, management and operational security controls to ensure that the Government's security requirements are met. These controls are described in DHS Sensitive Systems Policy Directive (PD) 4300A and TSA Management Directive (MD) 1400 series security policy documents and are based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 standards.

A.2. The Contractor shall include this prospective clause in all subcontracts at any tier where the subcontractor may have access to “sensitive information” as defined in this prospective clause.

B. General Security Responsibilities for Contract Performance

B.1. The Contractor shall ensure that its employees follow all policies and procedures governing physical, environmental, and information security described in the various TSA regulations pertaining thereto, good business practices, and the specifications, directives, and manuals for conducting work to generate the products as required by this contract. Personnel will be responsible for the physical security of their area and government furnished equipment (GFE) issued to them under the provisions of the contract.

B.2. All Contractor employees shall receive initial TSA IT Security Awareness Training within 60 days of assignment to the contract. The Government will provide the training via compact disc (CD) as necessary. The contractor shall distribute and track the CDs and report the status of employee training before the 21st of every month.

B.3. Refresher training must be completed annually thereafter.

B.4. Role Based training for contract employees individuals with Significant Security Responsibility (SSR), whose job proficiency is required for overall network security within TSA, will be in accordance with DHS and TSA policy. The contractor shall attend monthly ISSO training provided by the Government. The contractor is required to take privileged user training provided by the Government prior to being granted a privileged user account. The contractor shall track and report ISSO and privileged user training monthly.

a. A person who is a privileged user or, who has access to a privileged account, is considered to have SSR.

i. Privileged User - A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. Privileged users will have separate accounts from their standard user accounts in order to perform privileged access.

ii. Privileged Account - An information system account with approved authorizations of a privileged user. The following is an example of privileged users, accounts, role types, Privileged Access Request (PAR) status, and TSA status:
b. Individuals with SSR will have a documented individual training and education plan, which will ensure currency with position skills requirements, with the first course to be accomplished within 90 days of employment or change of position. The individual training plan will be refreshed annually or immediately after a change in the individual’s position or related position description requirements.

c. The education and training will meet standards established by the NIST and set forth in DHS and TSA security policy.

d. Evidence of training provided to personnel will be available upon request of the DHS IT Security Training Office, or during DHS/TSA onsite validation visits performed on a periodic basis.

B.5. All privileged Transportation Security Equipment (TSE) users shall be vetted by TSA’s Personnel Security Division. For example, the privileged users with “Z” accounts associated with TSE super user access. Privileged accounts shall be audited by IAD during Privileged Account Audits annually. Privileged users shall use Personal Identity Verification (PIV) cards issued by TSA to access the TSE. Vendors will be required to make their TSE compatible with TSA-issued PIV. As an interim standard to PIV authentication controls, the OSC ISSO shall determine and enforce the frequency for changing passwords or PINs as appropriate in accordance with appropriate guidance documentation (if published). In the absence of specific guidance documentation, passwords or Personal Identification Numbers (PINs) shall not remain in effect longer than ninety (90) days. The contractor shall adhere to additional password requirements in TSA Technical Standard (TS) TS-001, Passwords and Personal Identification Numbers (PINs).

B.6. The OEM will be required to have a designated Information System Security Officer (ISSO) to coordinate with TSA Office of Security Capabilities (OSC) ISSO on IT Security issues and compliance. The OEM ISSO will be responsible for developing all artifacts required to maintain the current security baseline. The OEM ISSO shall maintain the baseline, track changes that impact the security posture of the TSE and perform Ongoing Authorization and Continuous Diagnostics and Mitigation (CDM) to ensure active compliance with security requirements.
C. Configuration Management (hardware/software)

C.1. Hardware or software configuration changes shall be in accordance with the DHS Information Security Performance Plan (current year and any updates thereafter), the DHS CDM Program to include dashboard reporting requirements and TSA’s Configuration Management policy. The TSA Chief Information Security Officer (CISO)/ Information Assurance and Cyber Security Division (IAD) must be informed of and involved in all configuration changes to the TSA IT environment including systems, software, infrastructure architecture, infrastructure assets, and end user assets. The TSA OSC IT Security POC will approve any request for change prior to any development activity occurring for that change and will define the security requirements for the requested change.

C.2. The Contractor shall ensure all application or configuration patches and/or Request for Change (RFC) have approval by the Government Configuration Board and lab regression testing prior to controlled change release under the security policy document, TSA Management Directive (MD) 1400.3 and TSA Information Assurance Handbook, unless immediate risk requires immediate intervention. Approval for immediate intervention (emergency change) requires approval of the TSA OSC IT Security POC, SCCB co-chairs, and the appropriate Operations Manager, at a minimum.

C.3. The Contractor shall ensure all sites impacted by patching are compliant within 14 days of change approval and release.

C.4. The acquisition of commercial-off-the-shelf (COTS) Information Assurance (IA) and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting “sensitive information”) shall be limited to those products that have been evaluated and validated, as appropriate, in accordance with the following:

- The NIST Federal Information Processing Standards (FIPS) validation program.
- The National Security Agency (NSA)/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program.

C.5. US Government Configuration Board and DHS Configuration Guidance

a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the US Government Configuration Board (USGCB) and in accordance with DHS and TSA guidance.

1. USGCB Guidelines:

2. DHS Sensitive Systems Configuration Guidance
   a. Link to be provided later.

b) The standard installation, operation, maintenance, updates and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The
information technology should also use the Windows Installer Service for installation to the default “program files” directory and should be able to silently install and uninstall.

c) Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

d) The Contractor shall establish processes and procedures for CDM of Contractor systems that contain TSA data by ensuring all such devices are monitored by, and report to, the TSA Security Operations Center (SOC). Vendors shall report incidents immediately to the TSA Single Point of Contact (SPOC) at 1-800-253-8571 and TSA-CSIRT@tsa.dhs.gov.

C.6. All TSE shall be compliant with the approved DHS Hardening Guidelines for the platform on which they are being developed. In the absence of DHS hardening requirements, the contractor shall refer to NIST and the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG). Specific detailed guidance and process of information security requirements can be found in the SOP 1401 Plan of Action and Milestone (POA&M) Process, as well as the DHS 4300A PD Attachment H Plan of Action and Milestones (POA&M) Process Guide. Specific guidance for a Waiver may be found in SOP 1403 Waivers, as well as in the DHS 4300A Policy Directive Attachment B Waiver Request Form.

C.7. For TSE that use Operating Systems for which the Government has an Anti-Virus (AV) server, TSE shall include TSA-approved AV software configured to receive digitally signed automatic AV virus definition file updates from the TSA AV servers without interaction from the user or disruption to the system. The TSE needs to be STIP-enabled before this can be implemented and appropriate testing needs to occur at the TSA Systems Integration Facility (TSIF) before implementation. TSE that are not connected shall be updated with AV signatures every 30 days.

C.8. For TSE that use Operating Systems for which the Government does not have a central AV server, the contractor shall provide the TSE Endpoint Protection to include Anti-Virus update status in the following format:

<table>
<thead>
<tr>
<th>Product Version (Targeting</th>
<th>Antivirus Vendor (Windows Defender)</th>
<th>Antivirus Vendor (Kaspersky)</th>
<th>Antivirus Vendor (McAfee)</th>
<th>Antivirus Vendor (Symantec)</th>
<th>Antivirus Vendor (Trend Micro)</th>
<th>Antivirus Vendor (Virus)</th>
<th>Antivirus Vendor (Eset)</th>
<th>Antivirus Vendor (F-Secure)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.20358.0000</td>
<td>10.0.20358.0000</td>
<td>10.0.20358.0000</td>
<td>10.0.20358.0000</td>
<td>10.0.20358.0000</td>
<td>10.0.20358.0000</td>
<td>10.0.20358.0000</td>
<td>10.0.20358.0000</td>
<td>10.0.20358.0000</td>
</tr>
</tbody>
</table>

TSE that do not receive automatic AV virus definition file updates shall be updated with AV signatures every 30 days.

D. Risk Management Framework

D.1. The Security Authorization and Ongoing Authorization Process in accordance with NIST SP 800-37 and SP 800-137 (current versions) is a requirement for all TSA IT systems, including general support systems (e.g., standard TSA desktop, general network infrastructure, electronic mail, etc.), major applications and development systems (if connected to the operational network or processing, storing, or transmitting government data). These processes are documented in the NIST Risk Management Framework. Ongoing Authorization is part of Step 6 “Monitoring” of
the Risk Management Framework. All NIST and DIACAP guidance are publicly available; TSA and DHS security policy is disclosed upon contract award.

D.2. A written authority to operate (ATO) granted by the TSA Authorizing Official (AO) is required prior to processing operational data or connecting to any TSA network. The contractor shall provide all necessary system information for the security authorization effort.

D.3. TSA will assign a security category to each IT system compliant with the requirements of FIPS 199 and assign security controls to those systems consistent with FIPS 200.

D.4. Unless the AO specifically states otherwise for an individual system, the duration of any Accreditation will be dependent on the FIPS 199 rating and overall residual risk of the system; the length can span up to 36 months.

D.5. The Security Authorization Package contains documentation required for Security Authorizations and Ongoing Authorization. The package shall contain the following security documentation: 1) Security Assessment Report (SAR), 2) Security Plan (SP) or System Security Authorization Agreement (SSAA), 3) Contingency Plan, 4) Contingency Plan Test Results, 5) Federal Information Processing Standards (FIPS) 199 Security Categorization, 6) Privacy Threshold Analysis (PTA), 7) E-Authentication, 8) Security Assessment Plan (SAP), 9) Authorization to Operate (ATO) Letter, 10) Plan of Action and Milestones (POA&M), and 11) Ongoing Authorization Artifacts as required by the DHS Ongoing Authorization Methodology (current version). The SA package shall document the specific procedures, training, and accountability measures in place for systems that process personally identifiable information (PII). All security compliance documents will be reviewed and approved by the TSA Chief Information Security Officer (CISO) and the Information Assurance and Cyber Security Division (IAD), and accepted by the Contracting Officer upon creation and after any subsequent changes, before they go into effect.

D.6. Upon completion of security scans, findings will be documented and categorized as high, medium, or low based on their potential impact to the TSE IT Security posture. TSE contracts shall include engineering service hours to support the remediation of open POA&M items in a timely manner. High security findings must be remediated in 90 days or less; Medium security findings must be remediated in 120 days or less, and Low security findings must be remediated in 150 days or less. The OEM will work with the OSC ISSO and the respective Contracting Officer (CO) and/or Contracting Officer’s Representative (COR), as well as OIT IAD and the System Owner as required to prioritize and plan for the remediation of open POA&Ms. The OEM ISSO shall create and maintain all security artifacts and perform Ongoing Authorization (per NIST 800-137 and DHS-TSA requirements) and CDM (per OMB M-14-03) activities to ensure active compliance with security requirements.

E. **Contingency Planning**

E.1. The Contractor shall develop and maintain a Contingency Plan (CP), to include a Continuity of Operation Plan (COOP), to address circumstances whereby normal operations are disrupted.

E.2. The Contractor shall ensure that contingency plans are consistent with template provided in the DHS Information Assurance Compliance System Tool. If access has not been provided
initially, the contractor shall use the DHS 4300A Sensitive System Handbook, Attachment K, *IT Contingency Plan Template*.

E.3. The Contractor shall identify and train all TSA personnel involved with COOP efforts in the procedures and logistics of the disaster recovery and business continuity plans.

E.4. The Contractor shall ensure the availability of critical resources and facilitate the COOP in an emergency situation.

E.5. The Contractor will test their CP annually.

E.6. The Contractor shall record, track, and correct any CP deficiency and any deficiency correction that cannot be accomplished within one month of the annual test will be elevated to the Information Assurance and Cyber Security Division (IAD).

E.7. The Contractor shall retain records of the annual CP testing for review during periodic audits.

E.8. The Contractor shall ensure the CP addresses emergency response, backup operations, and recovery operations.

E.9. The Contractor shall have an Emergency Response Plan that includes procedures appropriate to fire, flood, civil disorder, disaster, bomb threat, or any other incident or activity that may endanger lives, property, or the capability to perform essential functions.

E.10. The Contractor shall have a Backup Operations Plan that includes procedures and responsibilities to ensure that essential operations can be continued if normal processing or data communications are interrupted for any reason for an unacceptable period of time as described in the Statement of Work.

E.11. The Contractor shall have a Post-disaster Recovery Plan that includes procedures and responsibilities to facilitate rapid restoration of normal operations at the primary site or, if necessary, at a new facility following the destruction, major damage, or other major interruption at the primary site.

E.12. The Contractor shall ensure all TSA data (e.g., mail, data servers, etc.) is incrementally backed up on a daily basis.

E.13. The Contractor shall ensure a full backup of all network data occurs as required by the system’s availability security categorization impact rating per TSA Information Assurance policy.

E.14. The Contractor shall ensure all network application assets (e.g., application servers, domain controllers, Information Assurance (IA) tools, etc.) will be incrementally backed up as required to eliminate loss of critical audit data and allow for restoration and resumption of normal operations within one hour.

E.15. The Contractor shall ensure sufficient backup data to facilitate a full operational recovery within one business day at either the prime operational site or the designated alternate site will be stored at a secondary location determined by the local element disaster recovery plan.

E.16. The Contractor shall ensure that data at the secondary location is current as required by the system’s availability security categorization impact rating.
E.17. The Contractor shall ensure the location of the local backup repository and the secondary backup repository is clearly defined, and access controlled as an Information Security Restricted Area (ISRA).

E.18. The Contractor shall adhere to the DHS Security Architecture Guidance Volume 1: Network and System Infrastructure for the layout of the file systems, or partitions, on a system’s hard disk impacting the security of the data on the resultant system. File system design shall:

- Separate generalized data from operating system (OS) files
- Compartmentalize differing data types
- Restrict dynamic, growing log files or audit trails from crowding other data.

E.19. The contractor shall adhere to the DHS Security Architecture Guidance Volume 1: Network and System Infrastructure Design for the management of mixed data for OS files, user accounts, externally-accesses data files and audit logs.

F. Program Performance

F.1. The Contractor shall comply with requests to be audited and provide responses within three business days to requests for data, information, and analysis from the TSA Information Assurance and Cyber Security Division (IAD) and management, as directed by the Contracting Officer.

F.2. The Contractor shall provide support during the IAD audit activities and efforts. These audit activities may include, but are not limited to the following: requests for system access for penetration testing, vulnerability scanning, incident response and forensic review. This requires all administrative accounts, to include root level access when required to perform these activities.

F.3. The OEM ISSO shall create and maintain all security artifacts and perform Ongoing Authorization and CDM activities to ensure active compliance with security requirements.

G. Federal Risk and Authorization Management Program (FedRAMP)

If a vendor is to host a system with a Cloud Service Provider, the following shall apply:

G.1. **FedRAMP Requirements**: Private sector solutions will be hosted by a Joint Authorization Board (JAB) approved Infrastructure as a Service (IaaS) Cloud Service Provider (CSP) (http://cloud.cio.gov/fedramp/cloud-systems) and shall follow the Federal Risk and Authorization Management Program (FedRAMP) requirements. The Cloud Service Provider shall adhere to the following in addition to the FedRAMP requirements: Identity and entitlement access management shall be done through Federated Identity; SSI and PII shall be encrypted in storage and in transit as it is dispersed across the cloud; Sanitization of all TSA data shall be done as necessary at the IaaS, PaaS or SaaS levels; Cloud bursting shall not occur; TSA data shall be logically separated from other cloud tenants; All system administrators shall be U.S. citizens; TSA data shall not leave the United States; The cloud internet connection shall be behind a commercial Trusted Internet Connection that has EINSTEIN 3 Accelerated (E3A) capabilities deployed. These include but are not limited to the analysis of network flow records, detecting and alerting to known or suspected cyber threats, intrusion prevention capabilities and under the direction of DHS detecting and blocking known or suspected cyber threats using indicators. The E3A capability shall use the Domain Name Server Sinkholing
capability and Email filtering capability allowing scans to occur destined for .gov networks for malicious attachments, Uniform Resource Locators and other forms of malware before being delivered to .gov end-users.

G.2. **Private Sector System Requirements**: TSA shall conduct audits at any time on the private sector systems, and the system shall be entered into the TSA FISMA Inventory as a system of record using the Control Implementation Summary (CIS) provided by the Cloud Service Provider. Security artifacts shall be created and maintained in the DHS Information Assurance Compliance Tool (IACS). The private sector systems are required to go through the Security Authorization Process and the Risk Management Framework in accordance the Federal Information Systems Management Act and NIST SP 800-37 Rev. 1. The cloud internet connection shall be behind a commercial Trusted Internet Connection that has EINSTEIN 3 Accelerated (E3A) deployed. Security event logs and application logs shall be sent to the TSA SOC. Incidents as defined in the TSA Information Assurance 1400.3 Management Directive and Handbook shall be reported to the TSA SPOC 1-800-253-8571. DHS Information Security Vulnerability Management Alerts and Bulletins shall be patched within the required time frames as dictated by DHS.

**H. Information Assurance Policy**

H.1. All services, hardware and/or software provided under this task order must be compliant with DHS Sensitive System Policy Directive 4300A, TSA MD 1400.3 Information Technology Security Policy, TSA Information Assurance Handbook and Technical Standards.

H.2. The Contractor solution shall follow all current versions of TSA and DHS policies, procedures, guidelines, and standards, which will be provided by the Contracting Officer, including but not limited to:

- DHS Sensitive Systems Policy Directive (PD) 4300A
- DHS Sensitive Systems Handbook 4300A
- TSA MD 1400.3 Information Technology Security
- TSA Information Assurance Handbook
- TSA Technical Standards
- DHS IT Security Architecture Guidance Volumes 1, 2 and 3
- DHS/TSA Systems Engineering Lifecycle (SELC)
- DHS Information Security Performance Plan (current fiscal year)
- DHS Ongoing Authorization Methodology (current version)
- OMB M-10-28, M-14-03

H.3. Authorized use of TSA IT systems and resources shall be in accordance with the TSA Information Assurance Handbook.

**I. Data Stored/Processed at Contractor Site**
I.1. Unless otherwise directed by TSA, all storage of data must be contained within the resources allocated by the Contractor to support TSA and may not be on systems that are shared with other commercial or government clients.

J. Remote Access

J.1. The contractor remote access connection to TSA networks shall be considered a privileged arrangement for both Contractor and the Government to conduct sanctioned TSA business. Therefore, remote access rights must be expressly granted, in writing, by the TSA Information Assurance and Cyber Security Division (IAD).

J.2. The Contractor remote access connection to TSA networks may be terminated for unauthorized use, at the sole discretion of TSA.

K. Interconnection Security Agreement

If the service being supplied requires a connection to a non-DHS, Contractor system, or DHS system of different sensitivity, the following shall apply:

K.1. Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding/agreement, service level agreements or interconnection service agreements.

K.2. ISAs shall be reissued every three (3) years or whenever any significant changes have been made to any of the interconnected systems.

K.3. ISAs shall be reviewed and updated as needed as a part of the annual FISMA self-assessment.

L. SBU Data Privacy and Protection

L.1. The contractor must satisfy requirements to work with and safeguard Sensitive Security Information (SSI), and Personally Identifiable Information (PII). All support personnel must understand and rigorously follow DHS and TSA requirements, policies, and procedures for safeguarding SSI and PII. Contractor personnel will be required to complete Annual online training for SSI, Informational Security, and TSA Privacy training, which take approximately one hour each.

L.2. The contractor shall be responsible for the security of i) all data that is generated by the contractor on behalf of the TSA, ii) TSA data transmitted by the contractor, and iii) TSA data otherwise stored or processed by the contractor regardless of who owns or controls the underlying systems while that data is under the contractor’s control. All TSA data, including but not limited to PII, sensitive security information (SSI), sensitive but unclassified (SBU), and critical infrastructure information (CII), shall be protected according to DHS and TSA security policies and mandates.

L.3. TSA will identify IT systems transmitting unclassified/SSI information that will require protection based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information:
1. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2. (current version)

2. National Security Agency (NSA) Type 2 or Type 1 encryption. (current version)

3. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) 4300A Sensitive Systems Handbook). (current version)

L.4. The contractor shall maintain data control according to the TSA security level of the data. Data separation shall include the use of discretionary access control methods, VPN encryption methods, data aggregation controls, data tagging, media marking, backup actions, and data disaster planning and recovery. Contractors handling PII must comply with TSA MD 3700.4, Handling Sensitive Personally Identifiable Information (current version).

L.5. Users of TSA IT assets shall adhere to all system security requirements to ensure the confidentiality, integrity, availability, and non-repudiation of information under their control. All users accessing TSA IT assets are expected to actively apply the practices specified in the TSA Information Assurance Handbook and applicable IT Security Technical Standards.

L.6. The contractor shall comply with Sensitive Personally Identifiable Information (Sensitive PII) disposition requirements stated in the TSA Information Assurance Handbook, applicable Technical Standards and TSA MD 3700.4, Handling Sensitive Personally Identifiable Information.

L.7. The Contractor shall ensure that source code is protected from unauthorized access or dissemination.

L.8. CFE which stores or transmits data in support of this contract shall be encrypted at rest and in transit in accordance with the TSA Information Assurance Handbook. Data will be wiped immediately from CFE when it is no longer required to support the contract in accordance with sanitization and disposition procedures specified in the TSA Information Assurance Handbook. This includes but is not limited to encrypted thumb drives and laptops. The contractor shall follow CO direction on usage of particular thumb drives or other external hard drives to use with TSE.

M. Disposition of Government Resources

M.1. At the expiration of the contract, the contractor shall return all TSA information and IT resources provided to the contractor during the contract, and provide a certification that all assets containing or used to process TSA information have been sanitized in accordance with the TSA MD 1400.3, TSA Information Assurance Handbook and Technical Standards. The contractor shall certify in writing that sanitization or destruction has been performed. Sanitization and destruction methods are outlined in the NIST Special Publication 800-88 Guidelines for Media Sanitization, and TSA Technical Standard 046 IT Media Sanitization and Disposition. The contractor shall email signed proof of sanitization to the COTR. In addition, the contractor shall provide a master asset inventory list that reflects all assets, government furnished equipment (GFE) or non-GFE that were used to process TSA information.
M.2. All media with resident data (to include diskettes, optical discs, hard drives, flash media, etc.) containing sensitive information (FOUO, SSI, PII, etc.), including backup media and MEM, shall be placed in a secure location when not in use and throughout the media’s lifecycle from creation through sanitization. Refer to TS-002 Encryption.

M.3. TSA IT asset inventory lists shall be maintained and updated to reflect the current configuration, location, and owner of the affected assets throughout the sanitization process.

N. Special Considerations and Circumstances (if applicable)

Security Program Plan

N.1. For major agency Information Technology (IT) infrastructure support ranging in the total estimated procurement value (TEPV) of about $100 million or above or per TSA management’s request, the contractor may need to provide, implement, and maintain a Security Program Plan (SPP) based on the templates provided by the TSA Information Assurance and Cyber Security Division (IAD). This plan shall describe the processes and procedures that will be followed to ensure the appropriate security of IT resources that are developed, processed, or used under this contract. At a minimum, the contractor’s SPP shall address the contractor’s compliance with the controls described in NIST SP 800-53 (current version). The security controls contained in the plan shall meet the requirements listed in the TSA Information Assurance Handbook, Technical Standards and the DHS Sensitive Systems Policy Directive and Handbook 4300A (current versions).

N.2. The SPP shall be a living document. It will be reviewed and updated semi-annually to address new processes, procedures, technical or federally mandated security controls and other contract changes that affect the security of IT resources under contract.

N.3. The SPP shall be submitted within 30 days after contract award. The SPP shall be consistent with and further detail the approach contained in the offeror’s proposal or quote that resulted in the award of this contract and in compliance with the requirements stated in this clause.

N.4. The SPP, as accepted by the Contracting Officer and Information System Security Officer (ISSO), shall be incorporated into the contract as a compliance document. The Contractor shall comply with the accepted plan.

O. Passwords

O.1. The TSA OSC ISSO shall determine and enforce the frequency for changing passwords in accordance with all current versions of TSA and DHS policies, procedures, guidelines, and standards.

P. Multi-Factor Authentication

P.1. Multi-Factor Authentication shall be implemented to allow TSA employees and contractors access to the TSA and operating systems including remote access to TSA systems and TSE’s. Authentication systems are frequently described by the authentication factors that they incorporate. The three factors often considered as the cornerstone of authentication are:

- Something you know (for example, a password);
• Something you have (for example, an ID badge or a cryptographic key); and
• Something you are (for example, a voice print or other biometric measurement).

Authentication systems that incorporate all three factors are stronger than systems that incorporate only one or two of the factors. The system may be implemented so that multiple factors are presented to the verifier, or some factors may be used to protect a secret that will be presented to the verifier. For example, a hardware device that holds a cryptographic key might be activated by a password or the hardware device might use a biometric representation to activate the key. This type of device provides two-factor authentication, although the actual authentication protocol between the verifier and the claimant only proves possession of the key.

P.2. The Homeland Security Presidential Directive 12 (HSPD-12) requires the use of the Personal Identity Verification (PIV) credentials as the common means of authentication for access to TSA’s facilities, networks, and information systems. Personal Identity Verification (PIV) credentials shall be used as the primary means of logical authentication for TSA sensitive systems.

Q. End-of-Life (EOL) / End-of-Service (EOS) Policy
Q.1. The System Owner shall ensure that any hardware or software that is procured develops a full lifecycle plan based on the vendor’s established life and service expectancy of the product and total cost of ownership. Any new or existing product that will reach end-of-life (EOL)* within two (2) years and is part of a TSA FISMA IT System will require development of a remediation, upgrade, replacement and funding plan to remove the EOL item(s) from the TSA environment completely within that time frame. A plan of action and milestone shall be submitted for risk acceptance to the TSA CISO and AO in order to track remediation milestones appropriately.

*EOL / EOS - Defined as production and/or development, technical support, application updates, spare parts and security patches which are no longer available from the vendor.

R. Contractor Supply Chain
The contractor shall protect against supply chain threats in accordance with NIST Supply Chain Risk Management (SCRM).

The OEM ISSO shall:

a. Ensure the protection against supply chain threats as part of a comprehensive, defense-in-breadth information security strategy.

b. Ensure that risk management activities include addressing supply chain risks for the system’s current, and all subsequent lifecycle phases, and documenting this activity.
c. Ensure that supply chain risk is identified and evaluated prior to all contract awards, changes, and whenever supply chain threat information indicates the existence of unmitigated system, program, or mission risk.

d. Include requirements for hardware, software assurances and supply chain risk management prior to acquisition of any hardware or software products.

e. Ensure that COTS hardware and software products shall be analyzed for supply chain risk prior to acquisition activities that procure new products, upgrade existing products, or that will integrate these products with commercial services.

f. Assign an impact level (high, moderate, low) to each C.I.A. security objective and shall apply NIST SP 800-161 controls as tailored specifically to the security objective at the determined impact level.

g. Implement NIST SP 800-161 security controls, using the FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems methodology, based on the FIPS 199 impact level established for each C.I.A security objective.

h. Determine the systems level of risk introduced by the IT supply chain and whether the risk from the threat is sufficient to require the implementation of countermeasures.

i. Implement appropriate countermeasures, commensurate with the level of risk to protect against supply chain threats.

S. Asset Management and Inventory Control

S.1. Any CFE being utilized to perform services on behalf of the Government need to be inventoried and approved by the Government. The contractor shall comply with the Government process for Asset Management and Inventory control in accordance with TSA MD 200.57. The contractor shall submit an Asset Management and Inventory Control plan for all contractor furnished equipment (CFE) and government furnished equipment (GFE) including, but not limited to thumbdrives, laptops, mobile equipment, and external drives, which are used in support of this contract.

S.2. The contractor shall record and maintain accountable property records including, but not limited to, Information Technology equipment (having memory), digital cameras, and wireless mobile devices (WMD).

S.3. All property and equipment supporting the contract which is acquired as new property shall be recorded at the acquisition cost and shall include all other costs necessary to bring the asset to an
oler condition including, but not limited to, payments to vendors for freight, handling, storage, design, construction, and installation.

S.4. Property shall be maintained by the contractor’s Accountable Property Officer (APO).

S.5. All financial supporting documentation of any purchased capitalized property shall be sent to the COR within 30 days of procurement. Documentation and questions should be directed to the COR.

S.6. The contractor shall complete TSA Forms 251 and 251-1 for sensitive or accountable property as requested by the COR.

T. References

Department of Homeland Security Acquisition Regulation (HSAR)

NIST SP 800-37
NIST SP 800-53
NIST SP 800 137
NIST SP 800-161
http://csrc.nist.gov/publications/PubsSPs.html

NIST FIPS 199
NIST FIPS 200
http://csrc.nist.gov/publications/PubsFIPS.html

NIST SCRM
http://csrc.nist.gov/scrm/

DISA STIGs (in place of MIL-STD 972)
http://iase.disa.mil/stigs/Pages/index.aspx
U. CONTRACTOR EMPLOYEE ACCESS (JUN 2006)

CONTRACTOR EMPLOYEE ACCESS (JUN 2006)

(a) Sensitive Information, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security 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, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) “Information Technology Resources” include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a
favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

ALTERNATE I (2006)

When the contract will require contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer’s Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.
(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department’s Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

1. The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;

2. There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

3. The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

(End of clause)

ALTERNATE II (JUN 2006)

When the Department has determined contract employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to IT resources, add the following paragraphs:

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department’s Chief Security Officer or designee.

(h) Contractors shall identify in their proposals, the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

(End of clause)

H-XX Special Information Technology Contract Security Requirements

(a) Identification Badges. All Contractor employees shall be required to obtain and wear TSA identification badges when working in TSA facilities.

(b) Computer Access Agreement. All Contractor employees (users, managers, and operators of the TSA network) must sign TSA Form 1403, Computer Access Agreement. A copy of which
shall be provided to the TSA contracting officer’s technical representative for retention for the duration of the contract.

(c) Personnel Security.

(1) Privileged access users are individuals who have access to an information technology (IT) system with privileges of Administrator or above and have access to sensitive network infrastructure data. Privileged access users will be appropriately screened on entry into the privileged access position and the initial screening shall be refreshed every two years,

(2) Individuals terminating voluntarily or involuntarily from a Contractor performing under contract at TSA must have an exit briefing, conducted by a supervisory or management-level employee of the Contractor in order to identify and explain their post-employment responsibilities to the TSA.

(3) Records of exit interviews will be signed and maintained by the Contractor as part of the individual employment record for a period of not less than two years following the termination of the individual’s employment.

(4) The Contractor shall notify the Contracting Officer's Technical Representative and the Contracting Officer with proposed personnel changes. Written confirmation is required. This includes, but is not limited to, name changes, resignations, terminations, and reassignments to another contract.

(5) The Contractor shall notify the TSA, in writing of any requested change in access requirements for its employees no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to other company engagements. The Contractor shall provide the following information to TSA: full name, social security number, effective date, and reason for change.

(6) The Contracting Officer must approve all personnel replacements. Estimated completion of the necessary background investigation for employee access to government facilities and information systems is approximately 30 days from the date the completed forms are received (and acknowledged as complete) in the Security Programs Division.

(7) Failure of any Contractor personnel to pass a background investigation, without timely substitution that meets the contracts requirements, may be grounds for termination of the contract.

(d) Non-Disclosure Agreements.

(1) All TSA contractor employees and consultants must execute a DHS Form 11000-6, Sensitive But Unclassified Information Non-Disclosure Agreement (NDA) upon initial assignment to TSA and before being provided access to TSA “sensitive and/or mission critical information.”
original NDA will be provided to the TSA contracting officer’s technical representative for retention for the duration of the contract.

(2) The Contractor, and those operating on its behalf, shall adhere to the requirements of the nondisclosure agreement unless otherwise authorized in writing by the Contracting Officer.

(e) Performance Requirements.

(1) The Contractor shall not be liable for any injury to Government personnel or damage to Government property arising from the use of equipment maintained by the Contractor, unless such injury or damage is due to the fault or negligence of the Contractor.

(2) Contracting Officer’s Technical Representative (COTR) and IT Security Division shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.