AMS/FAST CHANGE REQUEST (CR) COVERSHEET

Change Request Number: 19-11

Date Received: 2/21/19

Title: Personnel Security Changes - Guidance

Initiator Name: Tim Eckert

Initiator Organization Name / Routing Code: Procurement Policy Branch, AAP-110

Initiator Phone: 202.267.7527

ASAG Member Name: Genesta Belton

ASAG Member Phone: 202.267.0332

Policy and Guidance: (check all that apply)

- ☐ Policy
- ☒ Procurement Guidance
- ☐ Real Estate Guidance
- ☐ Other Guidance
- ☐ Non-AMS Changes

Summary of Change:
Change of reference to SSE ("Servicing Security Element") to AXP organizational designation.

Reason for Change:
Consistency with CR 19-03A reflecting current Personnel Security organization.

Development, Review, and Concurrence:
Acquisition Policy

Target Audience:
Contracting and program office personnel

Briefing Planned: No.

ASAG Responsibilities: None.

Section / Text Location:
T3.14.1A.3e (2)(b)(ix)

The redline version must be a comparison with the current published FAST version.

- (●) I confirm I used the latest published version to create this change / redline

or

- ( ) This is new content

Links:
https://fast.faa.gov/docs/procurementGuidance/guidanceT3.14.1.pdf

Attachments:
Redline and final documents.

Other Files:
N/A

Redline(s):

Section Revised:

3.14.1 A 3 – Personnel Security

Procurement Guidance - (~~1/2019~~ 4/2019)

T3.14.1 Security Revised 1/2009

- A Security
  - 1 Facility/Security Revised 1/2019
  - 2 Information Security and Privacy Revised 1/2019
  - 3 Personnel Security Revised ~~1/2019~~ 4/2019
  - 4 Foreign Nationals Revised 1/2019
  - 5 Related Security Guidance and Tools Revised 10/2018
  - 6 Sensitive Unclassified Information Revised 10/2016
- B Clauses Revised 1/2009
- C Forms Revised 10/2017

T3.14.1 Security Revised 1/2009

A Security

1 Facility/Security Revised 1/2019

FAA Facility (per Order 1600.69C, FAA Facility Security Management Program, Appendix 1,#29) is defined as any building, structure, warehouse, appendage, storage area, utilities, and component, which, when related by function and location form an operating entity owned, operated or controlled by the FAA**.**

2 Information Security and Privacy Revised 1/2019

All systems and applications must undergo a Security Authorization as specified in FAA Order 1370.121 FAA Information Security and Privacy Program & Policy, as amended, and required by Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource (2016), and the Federal Information Modernization Security Act (FISMA) 2014. FAA Order 1370.121 as amended requires the use of the FAA Security Authorization Handbook, current version. The FAA Security Authorization Handbook provides the required guidance, process, and templates for conducting a Security Authorization and is based on the most current versions of the National Institute of Standards and Technology (NIST) Publications and Standards, Department of Transportation (DOT) Compendium and FAA Policies.

The Office of Information Security and Privacy (IS&P), Compliance Division, Assessment Branch(AIS-230) provides Security Authorization services to Office of Finance and Management (AFN) organizations and Lines of Businesses (LOBs) that have requested and funded these services.

FAA will further use the Information Security Continuous Monitoring (ISCM) objective to protect High Value Assets (HVAs) and ~~information .~~ information. FAA and Contractor responsibilities are further defined in AMS clause 3.14-9 “Information Security Continuous Monitoring (ISCM) and Forensics on Contractor Systems”.

Privacy. The Privacy Act provides safeguards for individual privacy when the FAA contracts for the design, development and/or operation of a system of records on individuals on behalf of the FAA to accomplish a program function. The Act requires that the contractor follow all of the rules on privacy that apply to the FAA.

An FAA employee may be criminally and/or civilly liable for violations of the Act. When the contract provides for operation of a system of records on individuals, contractors and their employees are considered employees of the FAA for purposes of the criminal penalties of the Act.

The Contracting Officer must review requirements to determine whether a contract will involve the design, development and/or operation of a system of records on individuals. If one or more of these tasks

will be required, the Contracting Officer must insure that the contract specifically identifies the system of records on individuals and the design, development and/or operation work to be performed. The statement of work must identify the FAA rules and regulations implementing the Privacy Act.

Privacy and Information Technology. Agencies must ensure that contracts for information technology address protection of privacy in accordance with the Privacy Act (5 U.S.C. 552a) and Part 24. In addition, each agency shall ensure that contracts for the design, development, and/or operation of a system of records using commercial information technology services or information technology support services include the following:

(a) Agency rules of conduct that the contractor and the contractor's employees shall be required to follow.

(b) A list of the anticipated threats and hazards that the contractor must guard against.

(c) A description of the safeguards that the contractor must specifically provide.

(d) Requirements for a program of FAA inspection during performance of the contract that will ensure the continued efficacy and efficiency of safeguards and the discovery and countering of new threats and hazards.

The Department of Transportation's implementing rules and regulations for the Privacy Act are contained at 49 CFR Part 10.

3 Personnel Security **Revised ~~1/2019~~ 4/2019**

a. *Definitions.*

(1) *Access*. The ability to physically enter or pass through an FAA area or a facility; or having the physical ability or authority to obtain FAA sensitive information, materials, or resources; or the ability to obtain FAA sensitive information by technical means including the ability to read or write information or data electronically stored or processed in a digital format such as on a computer, modem, the Internet, or a local-or wide area network (LAN or WAN). When used in conjunction with classified information, access is the ability, authority, or opportunity to obtain knowledge of such information, materials, or resources, in accordance with the provisions of Executive Order (EO)12968, Access to Classified Information.

(2) *Classified Acquisition*. An acquisition that consists of one or more contracts in which offerors would be required to have access to classified information (Confidential, Secret, or Top Secret) to properly submit an offer or quotation to understand the performance requirements of a classified contract under the acquisition or to perform the contract.

(3) *Classified Contract*. Any contract, purchase order, consulting agreement, lease agreement, interagency agreement, memorandum of agreement, or any other agreement between FAA and another party or parties that requires the release or disclosure of classified information to the contractor and/or contractor employees in order for them to perform under the contract or provide the services or supplies contracted for.

(4) *Classified Information*. Official information or material that requires protection in the interest of national security and is labeled or marked for such purpose by appropriate classification authority in accordance with the provision of Executive Order 12958, Classified National Security.

(5) *Contractor Employee*. A person employed as or by a contractor, subcontractor, or consultant ~~supporting FAA~~supporting FAA or any non-FAA person who performs work or services for FAA within FAA facilities.

(6) *Electronic Questionnaires for Investigations Processing (eQIP)*. Government system used to electronically process initial and subsequent background investigation requests.

(7) *FAA facility*. Any staffed or unstaffed building structure, warehouse, appendage, storage area, utilities and components, which when related by function and location form an operating entity owned, operated or controlled by FAA.

(8) *Foreign National*. Any citizen or national of a country other than the United States who has not immigrated to the United States and is not a Legal Permanent Resident (LPR) of the United States.

(9) *Immigrant Alien*. Any person not a citizen or national of the United States who has been lawfully admitted for permanent residence to the United States by the U.S. Citizen and Immigration Service (USCIS). (Refer to the Immigration and Nationality Act (INA)(8 United States Code 1101), Sections 101(a)(3) and (20).

(10) *Non-Immigrant Alien*. Any person not a citizen or national of the United States who has been authorized to work in the United States by the USCIS, but who has not been lawfully admitted for permanent residence. (~~Refer to~~Refer to the INA, Sections 101(a)(3) and (20).

(11) *Operating Office*. An FAA line of business, an office or service in FAA headquarters or an FAA division-level organization in a region or center, or any FAA activity or organization that utilizes the services and/or work of a contractor.

(12) *Quality Assurance Program*. A system that provides a means of continuous review and oversight of a program/process to ensure (1) compliance with applicable laws and regulations; (2) the products and services are dependable and reliable.

(13) *Resources*. FAA physical plant, sensitive equipment, information databases including hardware, software and manual records pertaining to agency mission or personnel.

(14) *Sensitive Information*. Any information which if subject to unauthorized access, modification, loss, or misuse could adversely affect the national interest, 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 EO or an Act of Congress to be kept secret in the interest of national defense or foreign policy. Sensitive data includes propriety data.

(15) *Sensitive Unclassified Information (SUI)*. Unclassified information withheld from public release and protected from unauthorized disclosure because of its sensitivity. Section 552a of Title 5, United States Code (the Privacy Act) identifies information, which if subject to unauthorized access, modification, loss, or misuse could adversely affect the national interest, the conduct of Federal programs or the privacy to which individuals are entitled.

(16) *Servicing Security Element (SSE)*. The FAA headquarters, region, or center organizational element responsible for providing security services to a particular activity. Note: This term no longer applies to personnel security where the AXP organizational designation is now used instead. The term still applies to information and facilities security.

(17) *Vendor Applicant Process (VAP)*. FAA system utilized to process and manage personnel security information for contractor personnel.

b. The National Industrial Security Program (NISP) was established by EO 12829, January 6, 1993, to protect the Government's classified information. The NISP Operating Manual (NISPOM) prescribes the requirements, restrictions, and other safeguards necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of Classified information released by the U.S. Government. NISPOM is available online at the NISP Library.

c. AMS Policy Section 3.5, Patents, Data, and Copyrights, contains policy for safeguarding classified information in patent applications and patents.

d. *Classified Information-Responsibilities of the Contracting Officer (CO).*

(1) Ensure that the Screening Information Request (SIR) and contract clearly identify the security, access, storage, and safeguarding requirements for contractor access to any Classified National Security Information (CNSI) as well as the highest level of access required. Additionally ensure that the contract documentation and processes comply with current NISP requirements.

(2) The CO must contact the Information Safeguards Division, AXF-200 and the responsible Office of Personnel Security (AXP) Division regarding FAA procedures and requirements for any contracting activity requiring contractor or potential contractor access to classified information, whether that information is owned by another agency or FAA. The responsible security organizations include the following:

(a) Headquarters – ASH Information Safeguards Division, AXF-200

(b) ASH Office of Personnel ~~Security (~~Security (National Capital, AXP-300; East, AXP-400; Central, AXP-500 and West, AXP-600). The William J. Hughes Technical Center (WJHTC) is under the security cognizance of AXP-400 for classified contracting processes.

(c) Mike Monroney Aeronautical Center (MMAC) ~~is~~ is under the security cognizance of AXP-500 for classified contracting processes.

(3) *Prescreening Information Request Phase.* COs should review all proposed Screening Information Requests (SIRs) to determine whether access to classified information may be required by offerors, or by a contractor during contract performance. If access to classified information may be required, the CO must comply with subparagraph d.(1) and d.(2) above.

(4) *SIR Phase.* COs must:

(a) Ensure the classified acquisition is conducted in accordance with the requirements of d.(1) and d.(2) above;

(b) Include appropriate security requirements and clauses in SIRs (see AMS Clause 3.14-1, Security Requirements, and its alternates); and as appropriate in SIRs and contracts when the contractor may require access to classified information. Requirements for security safeguards in addition to those provided in AMS Clause 3.14-1, Security Requirements, might be necessary in some instances; and

(c) Ensure the use of Contract Security Classification Specification, DD Form 254 when classified contracts are employed.

e. *Employment Suitability and Security Clearances for Contractor Personnel.* FAA's policy on personnel security for contractor employees, including those working on a FAA contract employed at contractor facilities, requires that procurement personnel take appropriate actions to protect the Government's interest where it appears that contractor employees, subcontractors, or consultants may have access to FAA facilities, classified information, sensitive information, and/or resources. Additional details of the agency's contractor and industrial security program are provided in FAA Order 1600.72A.

(1) *Security Clearances for Contractor Employees.*

(a) FAA Orders 1600.2F and 1600.72A provide that contracts requiring contractor employees to have access to classified information must be prepared and processed according to the procedures contained in the National Industrial Security Program Operating Manual (NISPOM)

(b) In the case of a contract or agreement where the FAA requires persons not employed by the U.S. Government to have access to classified information, a

statement to that effect should be included in the SIR and the requirements of FAA Order 1600.72A.

(2) *Employment Suitability of Contractor Employees.*

(a) FAA Order 1600.72A provides specific guidance for determining suitability of FAA contractor employees for access to FAA facilities, classified information, Sensitive Unclassified ~~Information(~~Information (SUI), and/or network information systems. It outlines risk levels and associated investigations requirements, and identified additional specific requirements and exemptions from investigative requirements.

(b) As it pertains to suitability determinations, at a minimum, the following actions are required:

(i) Each SIR should include provisions that require the contractor to submit an interim-staffing plan describing the anticipated positions and key employees, as appropriate.

(ii) CO and the appropriate SSE, with input from the Operating Office (e.g., Contracting Officer's Representative (COR), have the responsibility to make an initial determination as to the applicability of the order in any given SIR and/or contract. An assessment will be made up-front as to whether any positions contained in the staffing plan will require access to FAA facilities, sensitive information, and/or resources. If the CO determines that the order does not apply to a given SIR/contract, this will be documented in a memorandum to file, indicating the matter was given due consideration, addressed adequately, and said determination made.

(iii) The Operating Office, in coordination with the COR, has the responsibility to make initial position risk/sensitivity level designations based on the initial list of positions and the Statement of Work (SOW). FAA Order 1600.72A contains information on designating position risk/sensitivity levels~~..~~. The Office of Personnel Management's Position Designation Automated Tool at https://www.opm.gov/suitability/suitability-executive-agent/position-designation-tool/#url=Automated-Tool was created to ensure positions are designated uniformly and consistently. It is to be used by the FAA Program Manager or Contracting Officer's Representative (COR) in conjunction with this process and to document the designations for all new contract awards. All OPM Position Designation Records must be submitted along with the Statement of Work to AXP for review and approval.

(iv) For modifications to existing contracts that change the security posture of the contract, new Position Designation Records must be completed and sent to the appropriate AXP office for review and approval. Modifications that do not affect the security posture do not require completion of new Position Designation Records prior to the execution of the modification. For new

contracts, the same process would be followed for determining risk/sensitivity level designations, using information required by way of a provision in the SIR.

(v) AMS Clause 3.14-2 will require the contractor to submit the completed documentation for each employee in a stated position, as necessary to permit the Office of Personnel Security to make an employment suitability determination. This documentation must be submitted through applicable systems or directly to ~~the appropriate~~the appropriate AXP office (for Privacy Act reasons) for approval, or denial of access, using the process described in FAA Order 1600.72A.

(vi) For new contracts, contractor employees must be required to submit the required documentation prior to performing or providing services or supplies under any FAA contract actions. Depending upon the nature and extent of access required, after an initial review of the documentation submitted by the contractor or contractor employee, AXP may grant interim suitability for the contractor employee to commence performing or providing services or supplies under the contract pending completion of the check and/or investigation and final suitability determination.

(vii) For modifications to existing contracts, contractor employees may continue working under the contract pending submission of the necessary documentation, if any, and completion of a background investigation by AXP, if required. Note there is a period of 30 days that cannot be exceeded in which contractors must submit the forms after the positions and ~~designated risk~~designated risk levels have been identified via contract modification. AXP may establish conditions governing such access pending completion of suitability investigation.

(viii) Notification of termination of employees performing within a stated position under a contract must be provided via the VAP to the FAA by the contractor within one (1) day.

(ix) COs will notify the appropriate AXP office whenever a contract is issued or when the status of a contract changes (i.e., replaced, defaulted, terminated, etc.). Prior coordination of new contracts should have occurred between the Operating Office, the CO, and ~~the SSE~~AXP.

(c) *Procedures for Processing Security Investigations*.

(i) Upon contract award, the CO or contractor will communicate to the personnel security specialist (PSS) a point of contact (POC) who will enter data into the Vendor Applicant Process (VAP) (vap.faa.gov). This POC should be a representative designated by the contractor, and each contract may have a maximum of 5 POCs per contract. The VAP administrator will provide a Web

ID~~, password~~, password to each POC and instructions how to operate the VAP system.

(ii) The following information must be entered by the POC into the VAP for each contractor employee requiring an investigation:

(AA) Name;

(BB) Date and place of birth (city and state); (CC)

Social Security Number (SSN);

(DD) Position and Office Location;

(EE) Contract number;

(FF) Current e-mail address and telephone number for applicant (personal or work); and

(GG) Any known information regarding current security clearance or previous investigations (e.g. the name of the investigating entity, type of background investigation conducted, contract number, labor category (Position), and approximate date the previous background investigation was completed).

(iii) The PSS will examine the information in VAP and check for prior investigations and clearance information.

(AA) If a prior investigation exists that meets the investigative requirements of the position, there has not been a 2-year break in service, and there is no new derogatory information known, the PSS will notify the vendor and CO/COR that no investigation is required and that final suitability is approved.

(BB) If no previous investigation exists, the PSS will send the applicant an e-mail:

(1) Stating that no previous investigation exists and the applicant must complete a form through the Electronic Questionnaires for Investigations Processing (eQIP) system;

(2) Instructing the applicant how to enter and complete the eQIP form;

(3) Providing where to send/fax signature and release pages and other applicable forms; and

(4) Providing instructions regarding fingerprints.

(iv) The applicant must complete the eQIP form and submit other applicable material within 5 days of receiving the e-mail from the PSS.

(v) If the eQIP form requires additional information, it will be rejected to the applicant with the reason for the rejection.

(vi) The PSS will notify the applicant and CO/COR of any interim suitability determinations.

(d) *Removal of Contractor Employees*. The POC, CO, or COR may notify AXP when a contractor employee is removed from a contract by using the Removal Entry Screen of VAP within 1 day of the removal.

(e) *Reports*. The POCs, COs, and CORs have the ability to run security reports from VAP for contracts and contractor employees.

f. *Costs of Investigations.* To pay for investigations, allotments of funds are made to regions, centers, and headquarters. Unless there has been a specific allotment to AXP to pay for all contractor employee investigations for operating officers that AXP services, each operating office must arrange to pay the costs for investigations on those employees working under contracts for which it is responsible. Security screenings, including fingerprint checks on contractor employees are funded through operational funds by each office or division. The operating office responsible for payment must provide AXP with the accounting code information necessary to have the cost charged appropriately.

g. *Contractor Off-Boarding Requirements*. Contractor employees departing from a FAA contract who have access to FAA facilities and/or Information Technology systems must each complete the FAA Contractor Employee Off-Boarding Checklist (see Procurement Forms). This does not apply to contractor employees who have been employed on the contract for less than six (6) months and have not been issued a yellow ID card.

The contractor employee's FAA sponsor is responsible for ensuring that the employee completes the Checklist. This responsibility may be delegated to the COR under a given contract. Contractor responsibilities are as indicated in AMS Clause 3.14-4 "Access to FAA Facilities, Systems, Government Property, and Sensitive Information".

4 Foreign Nationals **Revised 10/2017**

Foreign nationals employed or hired by the contractor to perform services for the FAA must have resided within the United States for three (3) years of the last five (5) years unless a waiver of

this requirement has been granted by AXP in accordance with FAA regulations (see AMS Clause 3.14-3, Foreign Nationals as Contractor Employees).

5 Related Security Guidance and Tools Revised 10/2018

The following sections refer to areas within the AMS Guidance that contain security issues to be considered during contract formulation.

T3.1.6 Nondisclosure of Information

T3.2.1 Procurement Planning

T3.2.2.5 Commercial and Simplified Purchase Method

T3.2.2.6 Unsolicited Proposals

T3.2.2.7 Contractor Qualifications

T3.3.1 Contract Funding, Financing & Payment

T3.5 Patents, Rights in Data, and Copyrights

T3.6.4 Foreign Acquisitions

6 Sensitive Unclassified Information Revised 10/2016

a. *General*.

(1) FAA Order 1600.75, "Protecting Sensitive Unclassified Information (SUI)," outlines policy and guidance on protecting sensitive unclassified information (SUI).

(2) When a contract, order, lease, or agreement requires a contractor or offeror to have access to SUI, the Contracting Officer (CO) must incorporate appropriate security clauses into the solicitation or contract. These include clauses on safeguarding standards, personnel security suitability, and non-disclosure agreements.

(3) SUI may include information such as Personally Identifiable Information (PII), sensitive NAS data, construction drawings, or equipment specifications. Prospective FAA vendors may need access to this information to ensure they can accurately propose and perform the work that FAA requires.

(4) When a screening information request (SIR) includes information determined to be SUI, the CO (and anyone else granted access to the SUI) must take reasonable care disseminating

the SUI documents and ensure the recipient has a *need-to-know* and is *authorized* to receive it.

b. *FOUO and SSI*. There are over 50 types of SUI; however the two types generally handled within FAA are:

(1) *For Official Use Only (FOUO).* FOUO is the primary designation given to SUI by FAA, and consists of information that could adversely affect the national interest, the conduct of Federal programs, or a person's privacy if released to unauthorized individuals. Uncontrolled issuance of FOUO may allow someone to:

(a) Circumvent agency laws, regulations, legal standards, or security measures; or

(b) Obtain unauthorized access to an information system.

(2) *Sensitive Security Information (SSI).* SSI is a designation unique to the FAA, DOT, and the Department of Homeland Security (DHS) Transportation Security Administration (TSA), and applied to information meeting the criteria of 49 CFR Part 15, Part 1520 and Subpart A. SSI is information obtained or developed while conducting security activities, including research and development. Unauthorized disclosure of SSI can:

(a) Constitute an unwarranted invasion of privacy;

(b) Reveal trade secrets or privileged or confidential information; or

(c) Be detrimental to transportation safety or security.

c. *Distribution of SUI Information*. When distributing SUI information, the CO (and anyone else granted access to the SUI, including prime contractors, subcontractors, suppliers, etc.) must ensure the persons receiving the information are *authorized* to receive the SUI and have a *need- to-know*. Methods of pre-award SUI dissemination utilized in FAA include FedBizOpps and hardcopy dissemination.

d. *Federal Business Opportunities (FedBizOpps).* FedBizOpps is an E-Gov initiative that provides a secure environment for distributing sensitive acquisition information (to include SUI) to vendors during the solicitation phase of procurement. This system electronically disseminates information or data to the vendor community while still protecting SUI from unauthorized distribution. Data that can be uploaded into FedBizOpps includes construction plans, equipment specifications, security plans, and SIRs. As FAA utilizes the FAA Contract Opportunities website to announce procurement opportunities, COs will utilize the Non-FBO Secure Document Link functionality in FedBizOpps when electronically distributing SUI.

(1) FedBizOpps provides several security measures to include:

(a) During processing of a vendor's access request to FedBizOpps, the vendor's profile is retrieved from the System for Award Management (SAM). Using the Data Universal Numbering System (DUNS) number, FedBizOpps ensures that the vendor seeking access is a viable vendor in SAM;

(b) *Marketing Partner Identification Number (MPIN).* A number required by FedBizOpps to access SUI. This number is unique to each vendor, and chosen by the vendor when each register with SAM;

(c) Vendors receive an e-mail after registration to confirm the validity of their identity and contact information;

(d) The access level of the data in FedBizOpps can be adjusted; the CO can specifically allow access to only certain vendors, or if a vendor requests access to the data and they are not specifically authorized, the system will verify with the CO if access should be granted (termed "Explicit Access Request");

(e) *Export Control.* When export control is selected in FedBizOpps, the system requires that the vendor be certified by the Defense Logistics Information Service Joint Certification Program before SUI will be released. This is usually reserved for technology related to military or space application; and

(f) The system tracks which Government users and vendors access the data through FedBizOpps.

(2) Use of FedBizOpps requires the CO to adhere to the following process:

(a) Upload SUI files into the FedBizOpps website (http://www.fbo.gov) by the procurement request (PR) and solicitation numbers. Note that the problems may arise when uploading attachments greater than 100 mb.

(b) "Release" the solicitation: Prior to it being made available to anyone through FedBizOpps, the CO must determine the scope of vendors allowed to access the data and release the data for authorized viewing.

(c) Once established in FedBizOpps, the system provides the CO a web address to provide to vendors that will link authorized persons directly into the applicable data. The CO can email this link to individual vendors when access has been restricted, or can place it on a public announcement via the internet so, if properly registered, all interested parties may view the data. Prior to downloading the data, the vendor must electronically sign an SUI policy statement in FedBizOpps.

(3) Web-based training and user guides are available to both FAA users and contractors at http://www.fbo.gov.

e. *Hardcopy Dissemination of SUI Using FedBizOpps*. At times, electronic versions of documents or data do not exist, and the SUI must be disseminated in a hardcopy form. In situations such as this, the CO must still utilize FedBizOpps for vendor verification and for the vendor to electronically read and certify to SUI policy. This will eliminate the need for the CO to manually validate vendor information and document in hardcopy form the vendor's certification to properly handle and protect SUI. Once the vendor is verified by FedBizOpps and has agreed to the SUI policy, the hardcopy documentation can then be forwarded to that vendor. Processes for distributing SUI in hardcopy form to vendors are:

(1) The CO may upload a "Document Security Notice and SUI Request Form" into FedBizOpps for the vendor to download, complete, sign, and return to the CO requesting the SUI data. Because the form can only be accessed after vendor verification and certification to SUI policy has taken place, hardcopy documentation can be distributed to the vendor after the CO receives a completed form. In some situations a portion of the SUI may be available in digital media and the remainder in hardcopy form; the CO may upload into FedBizOpps the digital portion for the vendor to download directly and the request form for the vendor to request the remaining hardcopy documentation; or

(2) The CO may request the vendor to use the "CD" link for hardcopy SUI documentation. Once the vendor links to the SUI, has properly accessed FedBizOpps, and certified to SUI policy, they may select the "CD" link. Once the vendor selects the link, the system sends the CO an e-mail with the vendor's information and request for the SUI. This link can be used for both hardcopy documentation and information that the CO desires to distribute via a CD or other like media. f. *Registration with FedBizOpps*.

(1) The process in which a CO registers for FedBizOpps is:

(a) Access the FedBizOpps website at http://www.fbo.gov.

(b) Click the "Register Now" link for buyers.

(c) Enter name, position, and e-mail information.

(d) Use the Agency drop-down menu to select the proper agency from the list provided. FAA users will select Department of Transportation/Federal Aviation Administration (FAA) for “Agency,” and the proper FAA location in which the user resides for the “Contracting Office Location.” The location list for FAA includes Headquarters and each region and center.

(e) Select the type of user account required. COs will choose Buyer from the menu.

Note: If a CO needs to release solicitations and post SUI in FedBizOpps, the CO must register for buyer and engineer user rights. The user rights of an engineer allow for

the posting of SUI, while those of the buyer group does not; however, the system does allow for a single user to have the rights of both user groups.

(f) Complete the remaining fields.

(g) Once the user clicks submit, the registration request is sent to the Administrator at DOT for processing. When approved, the user will receive an e- mail stating the result of the request and the appropriate username and password to use with FedBizOpps.

(2) The process in which a vendor registers in FedBizOpps is:

(a) Access the FedBizOpps website at http://www.fbo.gov.

(b) Click the "Register Now" link for vendors.

(c) The vendor will enter their DUNS Number for authentication.

(d) The vendor will review/update information retrieved from SAM, and enter other information to include a user name and password.

(e) Once submitted, the registration is analyzed and authenticated. If approved, the vendor will receive a confirmation page via e-mail detailing key information for FedBizOpps.

g. *Other Electronic Transfer and Dissemination*. Transfer and dissemination of SUI information beyond the intranet (internet or extranet, modem, DSL, wireless, etc.) must use at least 128 bit symmetric key encryption following NIST Special Publication 800-21 *Guideline For Implementing Cryptography in the Federal Government*. All transfers must use standard commercial products (such as PGP and Secret Agent) with encryption algorithms that are at least 128 bit symmetric (3DES, AES, RC4, IDEA, etc.), and follow the instructions outlined in this order. Authorized users that use project extranets for electronic project management during or after contract award to transfer SUI information are responsible for verifying and certifying to the CO that project extranets meet applicable physical and technical security requirements as determined by the Chief Information Officer. Access to the sites must be password protected and access must be granted only on a need-to-know basis. A record of those individuals who have had electronic access must be maintained by the CO or other disseminator in accordance with the system of keeping long-term records.

h. *Record Keeping*. Those who disseminate SUI information must obtain a signed "Document Security Notice and SUI Request Form" from anyone who receives the information (except for those vendors that utilize FedBizOpps for electronic data). Records of the signed forms must be maintained by the disseminator and destroyed 2 years after final disposition of the related SUI material (FAA Order 1350.15C and GRS 18 Item 1). At the completion of work, secondary and other disseminators must turn over their dissemination records to FAA, to be kept with the permanent files. The only records that the CO must keep for those vendors that utilize FedBizOpps to request SUI are the request forms for hardcopy documentation and any documentation detailing subsequent dissemination

by the vendor and their subcontractors or suppliers. Records of those who accessed SUI information via FedBizOpps and their associated SUI policy certifications are stored in FedBizOpps itself.

i. *Retaining and Destroying Documents*. The requirements above must continue throughout the entire term of contract and for whatever specific time thereafter as may be necessary. Necessary record copies for legal purposes (such as those retained by the architect, engineer, or contractor) must be safeguarded against unauthorized use for the term of retention. Documents no longer needed must be destroyed (such as after contract award, after completion of any appeals process, or completion of the work). Destruction must be by burning or shredding hardcopy, and physically destroying CDs, deleting and removing files from electronic recycling bins, and removing material from computer hard drives using a permanent erase utility or similar software.

j. *Notice of Disposal*. For all contracts using SUI, the contractor must notify the CO that it and its subcontractors have properly disposed of the SUI documents, except the contractor's record copy, at the time of Release of Claims to obtain final payment.

k. *State and Local Governments*. To comply with local regulations, FAA must provide localities with documents to issue building permits and to approve code requirements. Public safety entities such as fire departments and utility departments require unlimited access on a need-to- know basis. These authorities must be informed at the time they receive the documents that the information requires restricted access from the general public. When these documents are retired to local archives, they should be stored in restricted access areas. This will not preclude the dissemination of information to those public safety entities.

l. *Proprietary Information Owned by Architect/Engineers*. All professional services consultants must sign the "Document Security Notice and SUI Request Form" that documents containing SUI created under contract to the Federal Government must be handled according to the procedures under this guidance.

m. *Private Sector Plan Rooms*. Numerous private sector businesses provide plan rooms, which provide access to construction plans and specifications for bidding purposes as a service to construction contractors and subcontractors. Before receiving SUI from any source for dissemination, the private sector plan room must demonstrate to FAA that they will adhere to the procedures outlined this guidance, and sign the "Document Security Notice and SUI Request Form."

B Clauses **Revised 1/2009**

view contract clauses

C Forms **Revised 10/2017**

view procurement forms

The following security forms apply to FAA procurement:

- *DD Form 254* – *Contract Security Classification Specification*: For use by FAA personnel when classified contracts are employed.