

CHANGE REQUEST COVER SHEET

Change Request Number: 13-03

Date Received: 10/15/2012

Title: Personnel Security & Position Designation

Name: Eugene Scott

Phone: 202-493-4639

Policy OR Guidance: Guidance

Section/Text Location Affected: T3.14

Summary of Change: The Office of Security and Hazardous Materials Safety (ASH), will implement new personnel security verification requirements applicable to bringing in contractors. To comply with the change, Procurement Guidance section T3.14 Security, and clause 3.14-2 Contractor Personnel Suitability Requirements will be updated to remove the references to use of FAA form 1600-77 and replace with use of the OPM position designation tool.

Reason for Change: To ensure compliance with OPM security requirements related to the approval of contractor personnel requesting unescorted access to government facilities or networks.

Development, Review, and/or Concurrence: AIN-400, AAP-100, AGC-500, AAQ Division contracts managers, Aeronautical Center contracting.

Target Audience: Contracting officers, CORs and FAA staff that request contractors who must have unescorted access to FAA facilities or access to an FAA network.

Potential Links within FAST for the Change: None

Briefing Planned: No

ASAG Responsibilities: Approve

Potential Links within FAST for the Change: None

Links for New/Modified Forms (or) Documents (LINK 1)

Links for New/Modified Forms (or) Documents (LINK 2)

Links for New/Modified Forms (or) Documents (LINK 3)

SECTIONS EDITED:

Procurement Guidance:

T3.14.1 Security

Security

Section 3 : Personnel Security [\[Old Content\]](#) [\[New Content\]](#) [\[RedLine Content\]](#)

SECTIONS EDITED:

Section 3 : Personnel Security

Old Content: Procurement Guidance:

T3.14.1 Security

Security

Section 3 : Personnel Security

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 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 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) *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. Immigration and Naturalization Service (INS). (Refer to the Immigration and Nationality Act (INA)(8 United States Code 1101), Sections 101(a)(3) and (20).

(9) *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 INS, but who has not been lawfully admitted for permanent residence. (Refer to the INA, Sections 101(a)(3) and (20).

(10) *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.

(11) *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.

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

(13) *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.

(14) *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.

(15) *Servicing Security Element (SSE)*. The FAA headquarters, region, or center organizational element responsible for providing security services to a particular activity.

(16) *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 <https://www.dss.mil/GW/ShowBinary/DSS/index.html>.

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) Comply with NISP requirements.

(2) The CO must contact the personnel security specialists in the local office regarding FAA procedures and requirements for any contracting activity requiring access to classified information, whether that information is owned by another agency or FAA. The responsible security organizations includes the following:

(a) Headquarters – ASI-200

(b) Regions – 700-designated organizations, such as "ASO-700"

(c) Technical Center – ACT-8

(d) Aeronautical Center – AMC-700

(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 Order 1600.72A provides 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, sensitive information, and/or resources. 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, with input from the CO, 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 guidelines with a systematic process of uniformly designating program, position risk, and sensitivity levels. FAA form 1600-77, Contractor Position Risk/Sensitivity Level Designation Record is used in conjunction with this process and to document the designations.

(iv) For modifications to existing contracts, the appropriate SSE will approve the Operating Office's initial position risk/sensitivity level designations prior to the execution of the modification and these positions and risk level designations should be included in AMS Clause 3.14-2 at the time the contract is modified. 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, with final positions and risk levels being inserted into Clause 3.14-2 at time of contract award.

(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 SSE to make an employment suitability determination. This documentation must be submitted through applicable systems or directly to the SSE (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, the SSE 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 suitability investigation by the SSE. Note there is a period of 30 days that cannot be exceeded in which contractors must submit the forms after the positions and associated risks have been identified via contract modification. The SSE 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 SSE 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.

(c) Procedures for Processing Security Investigations.

(i) Upon contract award, the CO or company 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 and password to each POC.

(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 and there has not been a 2 year break in service, 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 (with a copy to the CO or company):

(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 15 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 the SSE/PSS when a contractor employee is removed from a contract by using the Removal Entry Screen of VAP.

(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 the SSE to pay for all contractor employee investigations for operating officers that the SSE 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 the SSE with the accounting code information necessary to have the cost charged appropriately.

New Content: Procurement Guidance:

T3.14.1 Security

Security

Section 3 : Personnel Security

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 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 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) *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).

(9) *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 the INA, Sections 101(a)(3) and (20).

(10) *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.

(11) *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.

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

(13) *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.

(14) *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.

(15) *Servicing Security Element (SSE)*. The FAA headquarters, region, or center organizational element responsible for providing security services to a particular activity.

(16) *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) Comply with NISP requirements.

(2) The CO must contact the personnel security specialists in the local office regarding FAA procedures and requirements for any contracting activity requiring access to classified information, whether that information is owned by another agency or FAA. The responsible security organizations includes the following:

(a) Headquarters – ASI-200

(b) Regions – 700-designated organizations, such as "ASO-700"

(c) Technical Center – ACT-8

(d) Aeronautical Center – AMC-700

(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 Order 1600.72A provides 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, sensitive information, and/or resources. 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, with input from the CO, 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 guidelines with a systematic process of uniformly designating program, position risk, and sensitivity levels. The Office of Personnel Management's Position Designation Automated Tool is to be used in conjunction with this process and to document the designations for all new contract awards. The FAA form 1600.77 Contractor Position Risk/Sensitivity Level Designation may continue to be used for existing contracts.

(iv) For modifications to existing contracts, the appropriate SSE will approve the Operating Office's initial position risk/sensitivity level

designations prior to the execution of the modification and these positions and risk level designations should be included in AMS Clause 3.14-2 at the time the contract is modified. 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, with final positions and risk levels being inserted into Clause 3.14-2 at time of contract award.

(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 SSE to make an employment suitability determination. This documentation must be submitted through applicable systems or directly to the SSE (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, the SSE 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 suitability investigation by the SSE. Note there is a period of 30 days that cannot be exceeded in which contractors must submit the forms after the positions and associated risks have been identified via contract modification. The SSE 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 SSE 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.

(c) Procedures for Processing Security Investigations.

(i) Upon contract award, the CO or company 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 and password to each POC.

(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 and there has not been a 2 year break in service, 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 (with a copy to the CO or company):

(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 15 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 the SSE/PSS when a contractor employee is removed from a contract by using the Removal Entry Screen of VAP.

(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 the SSE to pay for all contractor employee investigations for operating officers that the SSE 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 the SSE with the accounting code information necessary to have the cost charged appropriately.

Red Line Content: Procurement Guidance:

T3.14.1 Security

Security

Section 3 : Personnel Security

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 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 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) *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. [ImmigrationCitizen](#) and [NaturalizationImmigration](#) Service ([INSUSCIS](#)). (Refer to the Immigration and Nationality Act (INA)(8 United States Code 1101), Sections 101(a)(3) and (20).

(9) *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 [INSUSCIS](#), but who has not been lawfully admitted for permanent residence. (Refer to the INA, Sections 101(a)(3) and (20).

(10) *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.

(11) *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.

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

(13) *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.

(14) *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.

(15) *Servicing Security Element (SSE)*. The FAA headquarters, region, or center organizational element responsible for providing security services to a particular activity.

(16) *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 <https://www.dss.mil/GW/ShowBinary/DSS/index.html>.

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) Comply with NISP requirements.

(2) The CO must contact the personnel security specialists in the local office regarding FAA procedures and requirements for any contracting activity requiring access to classified information, whether that information is owned by another agency or FAA. The responsible security organizations includes the following:

(a) Headquarters – ASI-200

(b) Regions – 700-designated organizations, such as "ASO-700"

(c) Technical Center – ACT-8

(d) Aeronautical Center – AMC-700

(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 Order 1600.72A provides 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, sensitive information, and/or resources. 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, with input from the CO, 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 guidelines with a systematic process of uniformly designating program, position risk, and sensitivity levels. ~~FAA form 1600-77, Office Contractor Position of Personnel Risk/Sensitivity Management's Level Position~~ Designation ~~Record Automated Tool~~ is to be used in conjunction with this process and to document the designations for all new contract awards. The FAA form 1600.77 Contractor Position Risk/Sensitivity Level Designation may continue to be used for existing contracts.

(iv) For modifications to existing contracts, the appropriate SSE will approve the Operating Office's initial position risk/sensitivity level designations prior to the execution of the modification and these positions and risk level designations should be included in AMS Clause 3.14-2 at the time the contract is modified. 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, with final positions and risk levels being inserted into Clause 3.14-2 at time of contract award.

(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 SSE to make an employment suitability determination. This documentation must be submitted through applicable systems or directly to the SSE (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, the SSE 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 suitability investigation by the SSE. Note there is a period of 30 days that cannot be exceeded in which contractors must submit the forms after the positions and associated risks have been identified via contract modification. The SSE 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 SSE 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.

(c) Procedures for Processing Security Investigations.

(i) Upon contract award, the CO or company 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 and password to each POC.

(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 and there has not been a 2 year break in service, 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 (with a copy to the CO or company):

(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 15 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 the SSE/PSS when a contractor employee is removed from a contract by using the Removal Entry Screen of VAP.

(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 the SSE to pay for all contractor employee investigations for operating officers that the SSE 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 the SSE with the accounting code information necessary to have the cost charged appropriately.
