

# CHANGE REQUEST COVER SHEET

**Change Request Number:** 09-27

**Date Received:** 12/30/2008

**Title:** Implementation of Paperless Processes for Security

---

**Name:** Jeffrey Baker

**Phone:** 202-493-5723

**Policy OR Guidance:** Guidance

**Section/Text Location Affected:** AMS Procurement Guidance T3.14.1

**Summary of Change:** Revision of security language to introduce new electronic security procedures.

**Reason for Change:** To implement new FAA Security standards and meet new OPM investigation requirements.

**Development, Review, and/or Concurrence:** AIN-400, AGC-500, AJA-43, AJA-431, ARC, ACT

**Target Audience:** FAA Acquisition Workforce

**Potential Links within FAST for the Change:** None

**Briefing Planned:** No

**ASAG Responsibilities:** None

**Potential Links within FAST for the Change:** None

**Links for New/Modified Forms (or) Documents (LINK 1)** [null](#)

**Links for New/Modified Forms (or) Documents (LINK 2)** [null](#)

**Links for New/Modified Forms (or) Documents (LINK 3)** [null](#)

## SECTIONS EDITED:

Procurement Guidance:

**T3.14.1 Security** [\[Old Content\]](#) [\[New Content\]](#) [\[RedLine Content\]](#)

Procurement Guidance:

*T3.14.1 Security*

*Security*

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

Procurement Guidance:

*T3.14.1 Security*

**Section B : Clauses** [\[Old Content\]](#) [\[New Content\]](#) [\[RedLine Content\]](#)

Procurement Guidance:

*T3.14.1 Security*

**Section C : Forms** [\[Old Content\]](#) [\[New Content\]](#) [\[RedLine Content\]](#)

## SECTIONS EDITED:

**T3.14.1 Security (Revision 4, July 2008)**

**Old Content:** Procurement Guidance:

**T3.14.1 Security (Revision 4, July 2008) New Content:** Procurement Guidance:

**T3.14.1 Security Red Line Content:** Procurement Guidance:

**T3.14.1 Security** ~~(Revision 4, July 2008)~~

---

### **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 a 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 the 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 in support of the FAA or any non-FAA person who performs work or services for the FAA within FAA facilities.

(6) FAA facility. Any manned or unmanned 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.

(7) 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). (Reference the Immigration and Nationality Act (INA)(8 United States Code 1101), Sections 101(a)(3) and (20).

(8) 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. (Reference the INA, Sections 101(a)(3) and (20).

(9) 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.

(10) 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.

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

(12) 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.

(13) 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.

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

b. The National Industrial Security Program (NISP) was established by (EO) 12829; January 6, 1993, for the protection of the Government's classified information. The NISP Operating Manual (NISPOM) prescribes the requirements, restrictions, and other safeguards that are 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 on the Internet at <http://www.dss.mil/isec/nispom.htm>.

c. Section 3.5, Patents, Data, and Copyrights of the FAA Acquisition Management System contains policy for safeguarding classified information in patent applications and patents.

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

(1) Comply with NISP requirements.

(2) The CO must contact the personnel security specialists in the local office regarding FAA procedures/requirements for any contracting activity requiring access to classified information, whether that information is owned by another agency or the 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 (SIR) 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 d. (1) and d. (2) above.

(4) *SIR Phase.* COs must:

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

(b) Include appropriate security requirements and decending clauses in SIRs (see 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 Clause 3.14-1, Security Requirements, might be necessary in some instances.

(c) COs should 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 Technical Representative (COTR), 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) The 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 directly to the SSE (for Privacy Act reasons) for approval, or denial of access using the process described in FAA Order 1600.72A.

(vi) The SSE will initially coordinate with the CO on the approval (completeness and accuracy) of the submitted forms, and then on the status of any checks or investigations required and final decision of employment.

(vii) 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 conditional approval 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. However, this initial or interim suitability determination will not be automatically made by the SSE. The Operating Office must request this determination in writing.

(viii) 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.

(ix) The contractor must be required to provide quarterly updates, reporting changes to the status of employment of any contractor employee. However, notification of termination of employees performing within a stated position under a contract must be provided within one (1) day.

(x) 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.

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 a 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 the 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 in support of the FAA or any non-FAA person who performs work or services for the 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 manned or unmanned 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). (Reference 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. (Reference 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, for the protection of the Government's classified information. The NISP Operating Manual (NISPOM) prescribes the requirements, restrictions, and other safeguards that are 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 on the Internet at <https://www.dss.mil/GW/ShowBinary/DSS/index.html>.

c. Section 3.5, Patents, Data, and Copyrights of the FAA Acquisition Management System contains policy for safeguarding classified information in patent applications and patents.

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

(1) Comply with NISP requirements.

(2) The CO must contact the personnel security specialists in the local office regarding FAA procedures/requirements for any contracting activity requiring access to classified information, whether that information is owned by another agency or the 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 (SIR) 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 d. (1) and d. (2) above.

(4) *SIR Phase.* COs must:

- (a) Ensure that the classified acquisition is conducted in accordance with the requirements of d. (1) and (2) above;
- (b) Include appropriate security requirements and descending clauses in SIRs (see 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 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 Technical Representative (COTR), 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](http://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/COTR 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/COTR of any interim suitability determinations.

(d) *Removal of Contractor Employees.* The POC, CO, or COTR 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 COTRs 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 a 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 the 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 in support of the FAA or any non-FAA person who performs work or services for the 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 manned or unmanned 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.

(78) *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). (Reference the Immigration and Nationality Act (INA)(8 United States Code 1101), Sections 101(a)(3) and (20).

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

(910) *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.

(1011) *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.

(1112) *Resources*. FAA physical plant, sensitive equipment, information databases including hardware, software and manual records pertaining to agency mission or personnel.

(1213) *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.

(~~13~~**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.

(~~14~~**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, for the protection of the Government's classified information. The NISP Operating Manual (NISPOM) prescribes the requirements, restrictions, and other safeguards that are 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 on the Internet at <https://www.dss.mil/isecGW/ShowBinary/nispomDSS/index.htm>.

c. Section 3.5, Patents, Data, and Copyrights of the FAA Acquisition Management System contains policy for safeguarding classified information in patent applications and patents.

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

(1) Comply with NISP requirements.

(2) The CO must contact the personnel security specialists in the local office regarding FAA procedures/requirements for any contracting activity requiring access to classified information, whether that information is owned by another agency or the 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 (SIR) 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 d. (1) and d. (2) above.

(4) *SIR Phase*. COs must:

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

(b) Include appropriate security requirements and ~~decending~~descending clauses in SIRs (see 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 Clause 3.14-1, Security Requirements, might be necessary in some instances; ~~and~~

(c) ~~COs should ensure~~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 Technical Representative (COTR)), 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) ~~The~~ 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) ~~The SSE will initially coordinate with the CO on the approval (completeness and accuracy) of the submitted forms, and then on the status of any checks or investigations required and final decision of~~

~~employment. (vii)~~ 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 ~~conditional approval~~ 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. ~~However, this initial or interim suitability determination will not be automatically made by the SSE. The Operating Office must request this determination in writing.~~

~~(viii)~~ 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~~ 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.

~~(ix)~~ viii) ~~The contractor must be required to provide quarterly updates, reporting changes to the status of employment of any contractor employee. However, notification~~ 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/COTR 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/COTR of any interim suitability determinations.*

*(d) Removal of Contractor Employees. The POC, CO, or COTR 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 COTRs 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.

---

## **Section B : Clauses**

**Old Content:** Procurement Guidance:

*T3.14.1 Security*

**Section B : Clauses**

### 3-14 Security

3.14-1 Security Requirements – Classified Contracts (July 2002)

3.14-1/alt 1 Security Requirements – Classified Contracts Alternative I (July 2002)

3.14-1/alt 2 Security Requirements – Classified Contracts Alternative II (July 2002)

3.14-2 Contractor Personnel Suitability Requirements (July 2002)

3.14-3 Foreign Nationals as Contractor Employees (July 2002)

3.14-4 Government-Issued Keys, Identification Badges, and Vehicle Decals (July 2002)

3.14-5 Sensitive Unclassified Information (SUI) (April 2003)

**New Content:** Procurement Guidance:

*T3.14.1 Security*

**Section B : Clauses**

[view contract clauses](#)

**Red Line Content:** Procurement Guidance:

*T3.14.1 Security*

**Section B : Clauses**

[3-14 Security](#)

3.14-1 Security Requirements – Classified Contracts (July 2002)

3.14-1/alt 1 Security Requirements – Classified Contracts Alternative I (July 2002)

3.14-1/alt 2 Security Requirements – Classified Contracts Alternative II (July 2002)

3.14-2 Contractor Personnel Suitability Requirements (~~July 2002~~ January 2009)

3.14-3 Foreign Nationals as Contractor Employees (~~July~~ April ~~2002~~ 2008)

3.14-4 Government-Issued Keys, Identification Badges, and Vehicle Decals (July ~~2002~~ 2008)

3.14-5 Sensitive Unclassified Information (SUI) (~~April 2003~~ July 2008)

---

**Section C : Forms**

**Old Content:** Procurement Guidance:

*T3.14.1 Security*

**Section C : Forms**

The following forms apply to security related procurements. Hard copies of these forms may be obtained from the Investigative Division of the Office of Civil Aviation Security (ASI-200) for headquarters contracts, from the –700 Office of Civil Security in the regions and the Aeronautical Center, and from the ACT-8 Office of Civil Aviation Security at the William J. Hughes Technical Center. The FAA Form 1600.77 may be obtained in electronic format via the FAST Toolset.

For use by FAA personnel in designating position risk/sensitivity levels for contractor employees:

- FAA Form 1600-77 – Contractor Position Risk Sensitivity Designation Level Record

For use by Contractors in complying with the contract positions:

- Standard Form (SF) 85P, Questionnaire for Public Trust Positions
- FD-258 Card (original fingerprint card shall be used)

FAST Version 01/2009

CR 09-27

p. 23

**New Content:** Procurement Guidance:

*T3.14.1 Security*

**Section C : Forms**

[view procurement forms](#)

The following security forms apply to FAA procurement:

- *FAA Form 1600-77 – Contractor Position Risk Sensitivity Designation Level Record:* For use by FAA personnel in designating position risk/sensitivity levels for contractor employees, and may be obtained in electronic format via the FAST Toolset (Procurement Forms).
- [DD Form 254](#) – *Contract Security Classification Specification:* For use by FAA personnel when classified contracts are employed.

**Red Line Content:** Procurement Guidance:

*T3.14.1 Security*

**Section C : Forms**

The following security forms apply to ~~security-related procurements. Hard copies of these forms may be obtained from the Investigative Division of the Office of Civil~~FAA  
Aviation~~procurement:~~

- ~~FAA Security~~Form (ASI~~1600~~-200) ~~for headquarters contracts, from the 77 –700 Office of Civil Security in the regions and the Aeronautical Center, Contractor and from the Position Risk Sensitivity ACT-8 Designation Office Level of Record: Civil Aviation Security at the William For use by FAA personnel in J-designating Hughes position Technical risk/sensitivity Center. levels The FAA for contractor Form employees, 1600.77 and~~ may be obtained in electronic format via the FAST Toolset. ~~For use by FAA personnel in designating position risk/sensitivity levels for contractor (Procurement employees: Forms).~~
  - ~~FAA DD Form 1600-77~~254 – ~~Contractor Position Risk Contract Sensitivity Designation Security Classification Level Specification: Record~~ For use by ~~Contractors in complying with the contract positions: Standard Form (SF) 85P, Questionnaire for Public Trust Positions FD-258 Card~~FAA (original personnel fingerprint card shall be when classified contracts are used)~~employed.~~
-