



## Acronyms, Abbreviations, and Definitions

NBIS Release Version: 4.0

Updated Date: 05/23/2022

File ID: REF-008

### Standard Forms

Form	Description
SF-85	Standard Form Number 85 – Questionnaire for Non-Sensitive Positions.
SF-85P	Standard Form Number 85P – Questionnaire for Public Trust Positions.
SF-85P-S	Standard Form Number 85P-S – Supplemental Questionnaire for Selected Positions.
SF-86	Standard Form Number 86 – The OPM’s Questionnaire for National Security Positions (QSP).
SF-87	Standard Form Number 87- The fingerprint card

### Software

Term	Description
Central Verification System (CVS)	The Central Verification System (CVS) is used to determine if there is an existing adjudication or investigation that meets the current need. It is the primary tool for facilitating reciprocal decisions, as required by Executive Orders, regulations, and policies. CVS contains information on security clearance, suitability, fitness, and Homeland Security Presidential Directive 12 (HSPD-12) Personal Identity Verification (PIV) credentialing determinations.
Defense Information System for Security (DISS)	DISS is an enterprise-wide solution for personnel security, suitability, and credentialing management for DoD military, civilian, and contractors. It is a web-based application, a platform providing secure communications between adjudicators, security officers, and components, allowing users to request, record, document, and identify personnel security actions.
eApp	e-App is a secure web-based automated system which facilitates timely, accurate processing of investigation requests to DCSA. Agencies initiate individuals into the system, the system then collects data from the individual based on the appropriate investigative questionnaire (SF 85, SF 85P, SF 85P-S, or SF 86), and finally agencies review and submit the investigative questionnaire electronically to DCSA or another Investigative Service Provider (ISP).
e-QIP	e-QIP is a web-based automated system that was designed to facilitate the processing of standard investigative forms used by DCSA and other Investigation Service Providers (ISP) when conducting background investigations for Federal security, suitability, fitness and credentialing purposes. e-QIP allows the user to electronically enter, update and transmit their personal investigative data over a secure internet connection to a requesting agency.





Term	Description
<b>Personnel Information Processing System (PIPS)</b>	The system previously used to act as a repository containing background investigation records of Federal employees, military personnel, and contractors.
<b>Position Designation Automated Tool (PDT)</b>	The PDT is an interactive tool on the OPM website. The process determines, through the evaluation of national security and suitability requirements, what type of investigation is required and the depth that an individual is screened for a position. In order to ensure a systematic, dependable, and uniform method of determining position designations, OPM provides the Position Designation Automated Tool (PDT) for those individuals within agencies charged with position designation responsibilities.

## Case Types

Term	Description
<b>Tier 1</b>	Investigation required for positions designated as low risk, non-sensitive, and for physical and/or logical access, pursuant to Federal Information Processing Standards Publication 201 and Homeland Security Presidential Directive-12, using Standard Form 85, or its successor form.
<b>Tier 2</b>	Investigation required for non-sensitive positions designated as moderate risk public trust, using Standard Form 85P, or its successor form.
<b>Tier 3</b>	Investigation required for positions designated as non-critical sensitive, and/or requiring Determination for "L" access or access to Confidential or Secret information. This is the lowest level of investigation acceptable for access to classified information, using Standard Form 86, or its successor form. Requires a 10-year reinvestigation. Formerly known as National Agency Check, Local Agency Check and Credit Check.
<b>Tier 3R</b>	T3R is the reinvestigation product required for the same Tier 3 position.
<b>Tier 4</b>	Investigation required for non-sensitive positions designated as high-risk public trust, using Standard Form 85P, or its successor form.
<b>Tier 4R</b>	The reinvestigation product required for the same Tier 4 positions.
<b>Tier 5</b>	Investigation required for positions designated as critical sensitive, special sensitive, and/or requiring Determination for "Q" access or access to Top Secret or Sensitive Compartmented Information (SCI), using Standard Form 86, or its successor form. Requires a 5-yr. reinvestigation. Formerly known as Single Scope Background.
<b>Tier 5R</b>	The reinvestigation product required for the same Tier 5 positions.
<b>National Agency Check (NAC)</b>	Spouse/Cohabitant National Agency Check
<b>Special Agreement Check (SAC)</b>	Fingerprint Special Agreement Checks





## Government Abbreviations

Term	Description
<b>Business Event Type Code (BETC)</b>	This is up to an eight-digit alphanumeric code that indicates the type of activity being reported (payments, collections, etc.). Some agencies are using DISB if receiving services and COLL if performing services. BETC determines the transaction effect on the TAS Fund Balance with Treasury. BETC replaces transaction codes and subclasses, but at a more detailed level.
<b>Extra Coverage Codes (EC)</b>	Standard Form 85, 85P and 86 - Extra coverage codes are used to request information or processing beyond the normal scope of the investigation. Agencies must request extra coverage when additional information is needed to help determine a person's qualifications, suitability, or security for a particular position. Certain codes require an agreement with DCSA, and some incur additional fees. This is an optional field.
<b>Federal Investigations Processing Center Codes (FIPC)</b>	Codes that indicate special processing needs for an investigation request.
<b>Intra-Governmental Payment and Collection (IPAC)</b>	An Agency Location Code (ALC) is assigned to your agency by the U.S. Department of Treasury. The IPAC System provides a standardized interagency fund transfer mechanism for Federal Program Agencies (FPAs). IPAC facilitates the intra-governmental transfer of funds, with descriptive data from one FPA to another.
<b>Investigative Service Provider (ISP)</b>	A governmental organization that is actively involved in conducting investigations.
<b>Security Office Identifier (SOI)</b>	An agency's Security Office is responsible for receiving completed investigation reports from DCSA, controlling the agency's cases, and making the suitability and security determinations on individuals being investigated for employment. Each Security Office is issued a unique alphanumeric four-character identifier from DCSA, the Security Office Identifier (SOI), which is used to identify the appropriate agency official who will receive case results, data, or other information from DCSA.
<b>Submitting Office Number (SON)</b>	DCSA assigns a unique four-character alphanumeric code, known as the Submitting Office Number (SON), to each office that requests investigations from DCSA. The SON identifies the office that initiates the investigation and is recorded in the appropriate Order Form (Agency Use Block) of the SF 85, SF 85P, SF 85P-S, and SF 86.
<b>Treasury Account Symbol (TAS)</b>	A financial code, assigned by the Department of the Treasury, comprised of many separate, component pieces/ sub-fields* totaling 27 alphanumeric characters; however, not all sub-fields apply to each fund account. Among other things, the financial code identifies the agency, the period of availability of funds, and a specific fund account.





## Adjudication and Vetting Terminology

Term	Description
<b>Access</b>	The ability or opportunity to obtain knowledge of classified or sensitive information.
<b>Additional Considerations</b>	Determine the extent to which an issue makes the applicant unsuitable or unfit.
<b>Adjudication Factors</b>	Derogatory information evaluated in review of background information.
<b>Adjudication Guidelines</b>	A set of rules/criteria used to determine a subject's Determination to obtain access to classified information.
<b>Compartments</b>	Sensitive Compartmented Information (SCI) is divided into control systems, which are further subdivided into compartments and sub-compartments. Compartments protect national intelligence sources, methods, or analytical processes and measures are additional control systems used to protect intelligence sources and methods or analytical procedures.
<b>Determination</b>	The type of clearance for which a subject may be considered; or the determination assigned for a type of clearance, (e.g. Secret, Interim Declined, Favorable).
<b>Disqualifier</b>	Undesirable quality that renders a subject unqualified for a privilege or clearance.
<b>DISS File</b>	A file containing the adjudicative result data that is sent to the Defense Information System for Security (DISS) of record.
<b>Exceptions</b>	Exceptions identify conditions that exist and may be either monitored or unmonitored (e.g. monitored conditions include providing financial credit bureau reports on a quarterly basis; unmonitored conditions).
<b>Homeland Security Presidential Directive 12 (HSPD-12)</b>	Directive to mandate a federal standard for secure and reliable forms of identification. US policy to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).
<b>Issue Event</b>	The event that occurred with a subject, which could negatively impact their security clearance status.





# Reference File



Term	Description
<b>Issue Tag</b>	The qualifying language NBIS uses to identify what type of issue(s) occurred within an issue event for a subject.
<b>Mitigators</b>	Explanations, reasons, qualities, or actions that lessen the gravity of the disqualifier.
<b>National Security Guidelines</b>	Single common criteria for all covered individuals (e.g., U. S. Government civilian and military personnel, consultants, contractors, etc.) who require individual or continued Determination for access to classified information or Determination to hold a sensitive position.
<b>Public Trust</b>	Positions at high and moderate risk levels.
<b>Suitability</b>	An indication of a subject's ability to perform a job; typically based on experience or education.
<b>Suitability Guidelines</b>	Guidelines that identify character traits and conduct, and are sufficient to decide whether employment or continued employment would protect the integrity or promote efficiency of the service of a covered applicant, appointee, and employees.







## NBIS Terminology

Term	Description
<b>Assignment Rules</b>	Assignment Rules control the prioritization of how cases are assigned to users in the system based on certain case and user attributes.
<b>Case Phase</b>	The Phase is the highest-level grouping to describe where the case is at in the overall workflow for the personnel vetting process. It communicates to users the type of work currently being done on the case. Examples of phases include Initiation, Review, Authorize, Investigation, Continuous Vetting, Adjudication, etc.
<b>Case Progression Engine</b>	The progression engine pushes the case forward to the next status based on business rules of how many CV Alerts or Leads with specific attributes have been closed.
<b>Case Status</b>	The Status of the case communicates the specific part of the workflow the case is at within a Phase. So, it is a more granular indication of the case progress compared to the phase.
<b>Form Routing</b>	Form Routing is the configuration of the workflow process for the Initiation, Review, and Authorize phase. The organization will select which organizations they want the case to be routed to in each phase.
<b>Order Form</b>	The Order Form (previously known as the AUB), is the group of fields needed to complete the Agency Request. In NBIS, the Order Form is used in the Initiation, Review, and Authorize Phases.
<b>Org Relationship</b>	Organizations can establish relationships with each other when one organization is completing the work within a phase for another organization.
<b>Organization</b>	A government entity and/or an investigation service provider that is used to initiate requests, receive requests, conduct investigations, and adjudicate cases.
<b>Organization Context</b>	Organization Context refers to when you are in the Org Management tab, you are viewing all the data within that page in the context of a specific organization. It does not necessarily apply to all organizations you are in.
<b>Owning Organization</b>	This is the organization that is actively providing the subject with a paycheck. They are responsible for maintaining the subject's Determination.
<b>Persona</b>	A user can have multiple personas within their profile. An example of when a persona might be used is when a user needs permissions for their federal and contractor profiles.
<b>Program Tags</b>	Used to label and place restrictions on cases to allow certain users to work on, view, or allow a case to appear on a list.





# Reference File



Term	Description
<b>Service Catalog</b>	Service Catalog requests are configurable case types to provide services for internal and external organizations.
<b>Servicing Organization</b>	An organization may have a servicing relationship with the subject if they need to be notified of a change in a person's Determination status or if they need to update their record.
<b>Sponsoring Agency</b>	A government department or agency that is sponsoring the subject's investigation request.
<b>SSC</b>	Security, Suitability, and Credentialing. In NBIS, SSC is an available Organization Type that gives the organization access to the Subject Management function.
<b>Subject</b>	An individual who is authorized to fill out the Standard Forms via the e-App system.
<b>Team</b>	A Team is a group of users within an organization, that is mainly created for organizational/management purposes and is not public facing. Example would be Army (Primary Organization) - Army Brigade (Sub-Organization) - Group A (Team within either Army or Army Brigade).
<b>User</b>	The different government or industry employees that will be utilizing the NBIS System.
<b>User Assignment Capabilities</b>	User capabilities tell the system the types of cases and amount of work a user can take on. They are used by the assignment engine to determine which cases to assign to which users.
<b>User Assignment Templates</b>	Users can create standard templates to use when completing users' assignment capabilities in their user profile for a more efficient way of filling out that information. User Assignments are what allow a user to work on cases with certain attributes.
<b>User Level</b>	User Levels are used to assign work to users based on their skill level. Examples could include Junior or Senior.
<b>Workbasket</b>	The workbasket refers to a task or case in an organization that is not assigned to a specific user yet. In Task Management, the My Team's Work or My Org's Work is equivalent to the workbasket.
<b>Workflow Builder Actions</b>	Actions are the driving component of the workflow. Actions can be available within multiple Statuses in the workflow; however, an Action can only be configured to end in a single Status. Actions can have one or multiple associated Modules. Action naming and configuration should communicate to the user what will occur when the Action is performed.
<b>Worklist</b>	The worklist refers to a task or case being assigned directly to a specific user. In Task Management, the My Work tab is equivalent to the user's worklist.

