

Glossary

Introduction to DOD HSPD-12 CAC Credentialing

Actionable Information: Information that may be disqualifying based on credentialing standards addressed later in the course.

Adjudication:

- Apply HSPD-12 credentialing standards to investigative results
- Make final CAC credentialing trust determination
- Hold due process proceedings (if applicable)
- Record the final credentialing trust determination

Applicant:

- Provide identification
- Complete application online
- Have fingerprints taken
- In-person visit to card issuing facility to receive CAC

CAC: Common Access Card

DCSA Adjudicator:

- Review applications and conduct initial review of background investigations
- Apply HSPD-12 credentialing standards
- Return case to Component Adjudicator for final decision, if unable to make a favorable credentialing trust determination

Case Closing Transmittal: The Case Closing Transmittal is the cover sheet and provides a summary of the results of the investigation.

Checks: The investigation includes the following types of checks:

- Security and Suitability Investigations Index (SII) – Investigations previously conducted by OPM or other non-DOD Federal investigative agencies
- Defense Central Index of Investigations (DCII) – Investigations previously conducted by DOD
- FBI National Criminal History Check – checks on criminal history, Social Security Administration, military service, and terrorist databases
- Local Agency Checks – Checks on history with law enforcement agencies covering applicant's employment, residence, and education

CHR: Criminal History Report

Component Adjudicator:

- Review applications and background investigations

- Apply HSPD-12 credentialing standards
- Make HSPD-12 temporary/interim or preliminary decisions
- Make final credentialing trust determination if CAS Adjudicator is unable to make a favorable trust determination

CVS: Central Verification System

- Owned and managed by OPM
- Stores information on investigations and adjudications
- Key to ensuring transfer of trust, formerly known as reciprocity

DCII: Defense Central Index of Investigations**DCSA:** Defense Counterintelligence and Security Agency**DEERS/RAPIDS:** Defense Enrollment Eligibility Reporting System/Real-Time Automated Personnel Identification System

- DEERS: definitive data source of DOD personnel identity verification
- RAPIDS: used to verify identity and issue the CAC

DISS/NBIS: Defense Information System for Security/National Background Investigation Services – Stores national security, suitability, fitness, and credentialing trust determinations

- Securely connects DOD security personnel around the world
- Stores national security adjudicative actions and determinations
- Contains a shell indicating whether investigation has been scheduled
- Includes records national security, suitability, and HSPD-12 credentialing determinations

DOD: Department of Defense**DOD Card Issuance Facility:**

- Use of DEERS/RAPIDS
- Conduct identity proofing and registration
- Issue CACs

DOD Manual 1000.13 Volume 1: DOD Manual 1000.13, Volume 1, which is called *DOD Identifications Cards: ID Card Life-Cycle*.**DODI 5200.46:** Department of Defense Instruction 5200.46: *DOD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)*.**eApp:** Electronic Application

- Automates application process
- Formerly known as e-QIP (Electronic Questionnaires for Investigations Processing)

FBI: Federal Bureau of Investigation

FIPS 201-3: Federal Information Processing Standards, or FIPS, 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors* requires, among other things, that agencies establish appeals procedures for those individuals who are denied credentials or whose credentials are revoked.

Form I-9: Department of Homeland Security, Employment Eligibility Verification

HSPD-12: Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors* (2004) sets government-wide standards for Personal Identity Verification (PIV) and ensured identification, resistance to fraud and tampering, and authentication.

Initial Vetting: Conducts the vetting needed to establish trust with an individual not previously vetted. This is the first step for an outsider to become a trusted insider and is designed to establish the trust relationship between the government and the individual.

Interim CAC Review:

- Verify investigation is scheduled
- Receive FBI National Criminal History Report
- Apply HSPD-12 credentialing standards
- Make temporary/interim or preliminary CAC credentialing determination

Investigation: Investigative Service Providers (ISPs) collect information and provide adjudicators with a report needed to support a trust determination.

- Gather information on the subject's background to meet the investigative requirements for obtaining a CAC
- Low Tier or greater required for HSPD-12

ISP: Investigative Service Provider

- In most cases, DCSA
- Conduct investigation
- Provide results to component

Logical Access: Logical access to DOD networks via login:

- Onsite using a computer with a government-controlled configuration
- Remotely using DOD-approved remote access procedures in accordance with the Defense Information Systems Agency (DISA) Security Technical Information Guide (STIG)

Low Tier: The minimum investigation required to be issued a CAC. It contains database checks and written inquiries.

Memorandum: Credentialing Standards Procedures for Issuing PIV Cards under HSPD-12 and New Requirements for Suspension or Revocation of Eligibility for PIV Credentials: This memorandum provides government-wide credentialing standards procedures to be used by all Executive Branch Departments and Agencies (D/As) in issuing, suspending, or revoking eligibility for HSPD-12 PIV credentials to their employees and contractor personnel, including those who are non-United States citizens.

NAC: National Agency Check

NIPRNet: The Non-Secure Internet Protocol Router Network (NIPRNet) is a global, long-haul Internet Protocol (IP)-based network to support classified IP data communications services for combat support applications in the Department of Defense.

OF-306: Optional Form 306, Declaration for Federal Employment

OMB M-05-24: Office of Management and Budget Memorandum M-05-24 (August 2005) directs that HSPD-12 credentialing adjudications be based on a National Agency Check with Inquiries (NACI) or an equivalent or greater employment or national security investigation.

OMB M-19-17: Office of Management and Budget Memorandum M-19-17 (May 2019) sets forth the Federal Government's Identity, Credential, and Access Management (ICAM) policy.

OPM: Office of Personnel Management

OPM FIN 10-05: Office of Personnel Management Federal Investigations Notice 10-05

Order of Operations: Trust determinations are made in the following sequence:

1. Suitability or fitness for trust determination, if applicable.
2. National security trust determination, if applicable.
3. Credentialing trust determination, if needed.

Physical Access: Physical access on a recurring basis to multiple DOD facilities and/or multiple non-DOD, federally controlled facilities on behalf of the DOD.

PIV: Personal Identity Verification

Pre-investigation:

- Determine requirement for CAC
- Identity proofing and registration
- Initiation of investigation
- Check for previous investigations
- Initiate Application
- Collect fingerprints
- Submit application to ISP

Preliminary Determination: Using the adjudicative criteria for the applicable personnel vetting domain(s) to assess the results of high-yield checks, Departments and Agencies may make a preliminary determination to onboard the individual, prior to completing the investigative coverage requirements and making the trust determination.

Presumptively disqualifying information: Information found in an applicant's SF-85, SF-85P or SF-86, OF-306, or FBI Criminal History Report that indicates that the individual should not receive a CAC until the full investigation is completed and a final trust determination can be made.

Re-establishment of Trust (RoT): Simplifies the re-entry of trusted insiders back into the workforce after a period away from government work.

Risk Assessment: Adjudicators will analyze investigative and/or developed information to determine the likelihood an individual presents or will present an unacceptable risk to people, property, information, or mission.

ROI: The Report of Investigation contains the results of the investigation.

SF-85: Standard Form 85, Questionnaire for Non-Sensitive Positions

SF-85P: Standard Form 85P, Questionnaire for Public Trust Positions

SF-86: Standard Form 86, Questionnaire for National Security Positions

SII: Security and Suitability Investigations Index

SSA: Social Security Administration

Support Documents: If there are any issues with the results of the investigation, such as with any of the checks or written inquiries, the supporting documentation is included in the ROI.

Tier 1: Low Tier. The minimum investigation required to be issued a CAC. It contains database checks and written inquiries.

Transfer of Trust (ToT): The acknowledgement and acceptance of a previous background investigation or continuous vetting activities conducted by an authorized personnel vetting ISP and/or a suitability, fitness, national security or credentialing trust determination made by an authorized adjudicative D/A. It occurs when a trusted insider moves between positions, departments, and/or agencies. This is previously known as *reciprocity*.

Trusted Workforce 2.0 Implementation and Operational-Level Guidance for Departments and Agencies and Authorized Investigative Service Providers: This memorandum established guidance to transition to a new three-tiered investigative model and addresses the legacy investigative products conducted under the 2012 FIS.

Upgrade: Quickly raises the level of vetting when an individual requires a higher level of trust.

Written Inquiries: The investigation includes written inquiries, regarding the applicant's employment history and educational history.