

CONTINUOUS EVALUATION

Frequently Asked Questions (FAQ)

OVERVIEW OF CONTINUOUS EVALUATION (CE)		
1.	What is Continuous Evaluation (CE)?	<i>CE is a personnel security investigative process that leverages automated record checks of commercial records, U.S. Government (USG) databases, and other information lawfully available to security officials, to continuously review the background of individuals who have been determined to be eligible for access to classified information or eligible to hold a sensitive position.</i>
2.	How does CE work? What information does CE query?	<i>The Information Technology (IT) capability to conduct frequent, automated checks of security-relevant information is fundamental to the CE process and assists in early identification of potential security concerns. The CE System (CES) applies standardized personnel security business rules to identify relevant information and generates electronic alerts that are delivered to agency personnel security officials. CES record checks help mitigate the risk posed by malicious insiders by identifying relevant information earlier and more frequently than occurs through manual record checks. CE data sources fall into seven categories, as prescribed by Security Executive Agent (SecEA) and Federal Investigative Standard (FIS) requirements: (1) clearance eligibility, (2) terrorism, (3) foreign travel, (4) suspicious financial activity, (5) criminal activity, (6) credit reports, and (7) commercial public records.</i>
3.	What was the impetus for CE?	<i>Implementing CE is a key component of the government-wide effort to modernize security clearance processes and increase the timeliness of information reviewed between periodic reinvestigation cycles. Mandated by Executive Order (E.O.) 13467, as amended, and 5 U.S.C § 11001, CE automated record checks are the cornerstone of the broader Continuous Vetting framework that is addressed by the ongoing Trusted Workforce initiative.</i>
4.	Who is subject to CE?	<i>Current Executive Branch personnel (including, but not limited to, contractors, subcontractors, licensees, certificate holders, grantees, experts, consultants, military personnel, and government employees) who have been determined to be eligible for access to classified information or to hold a sensitive position.</i>
5.	Did I authorize my participation in CE?	<i>Yes. In signing the Standard Form 86 (or equivalent forms) for release of information and submission to either an initial or periodic background investigation for the purpose of attaining a security clearance or hold a sensitive position, you have authorized the USG to conduct background investigations, reinvestigations, and continuous evaluation.</i>

6.	Does CE involve review of an individual’s social media activities?	<i>No. CE includes review of Publicly Available Electronic Information (PAEI) but does not include the review of social media. However, under the broader vetting process, security officials are authorized to collect publicly available social media information during background investigations pursuant to SecEA Directive 5, Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications.</i>
HOW WILL CE IMPACT ME?		
7.	I received a credit bureau notification stating the USG checked my credit. Does this affect my credit score?	<i>No. CE automated credit checks are categorized as employment “soft inquiries,” and soft inquiries do not affect a person’s credit score. The “hard inquiries” that negatively affect credit scores are conducted by retailers, financial institutions and other lenders.</i>
8.	How is my personal information protected from inappropriate use or unauthorized access under CE?	<i>Security officials evaluate clearance eligibility using standards that incorporate protections for privacy and civil liberties with adherence to existing policies for collection, safeguards, use, and disclosure of protected Personally Identifying Information (PII).</i>
9.	Are there additional personnel security and/or counterintelligence reporting requirements as a result of CE?	<i>No. Reporting requirements are determined by an individual’s department or agency in accordance with Director of National Intelligence (DNI) policy. See SecEA Directive 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position; and Intelligence Community Standard 703-02, Reporting Requirements for Individuals with Access to Sensitive Compartmented Information.</i>
10.	Can I opt out of CE?	<i>Yes, but this prevents your agency from revalidating your continued eligibility for access to classified information or to hold a sensitive position.</i>
11.	Will I still be enrolled in CE when I separate from government service?	<i>No. Individuals no longer affiliated with a government sponsor will be unenrolled and removed from the CE System.</i>
WHY IS CE IMPORTANT?		
12.	How does CE protect against the disclosure of classified information?	<i>There is no guarantee that CE record checks, or any other initiative, can prevent the unauthorized disclosure of classified information by malicious insiders. However, CE is one of many initiatives that enhances existing personnel security processes designed to recruit and retain a strong and trusted workforce.</i>
13.	Why doesn’t CE only focus on personnel in high risk positions with privileged access?	<i>The numerous incidents of unauthorized disclosure of classified information over the years underscore the fact that anyone—at any level of access to classified information—can pose a threat to national security.</i>

14.	What happens if derogatory information is identified during CE record checks?	<i>Derogatory information identified during CE automated record checks is used for investigative lead purposes only. SecEA Directive 6, Continuous Evaluation, stipulates that “[i]nformation gathered by CE shall be forwarded to the sponsoring agency for analysis of adjudicative relevance and a determination if the information meets thresholds for further investigation and/or adjudication. Authorized investigative agencies shall make reasonably exhaustive efforts to verify that any information collected that is discrepant or potentially disqualifying pertains to” the evaluated individual. No action will be taken based solely on information identified during the CE process without follow-up and review using established national security adjudicative guidelines.</i>
15.	What happens if CE identifies inaccurate information?	<i>Standard personnel security business processes are used to review, validate, and correct inaccurate information identified during CE record checks.</i>
16.	Will CE replace clearance reinvestigations?	<i>No; however, some periodic reinvestigations are deferred if no security-relevant issues exist and the individual is enrolled in CE. Under the broader government-wide Continuous Vetting framework developed by the Trusted Workforce 2.0 initiative, the reinvestigation requirement will remain but they will be performed based on an event- or risk-driven model rather than a calendar-driven model.</i>
17.	Where can I go for more information about CE?	<i>You can learn more about CE by visiting https://www.ncsc.ic.gov/issues/ce.html on JWICS or https://ncsc.gov on the UNCLASSIFIED network.</i>