



## PERSONNEL VETTING PROCESS

### Webcast Episode 4: Continuous Vetting

**NARRATOR:** Welcome to the Personnel Vetting Process Webcast. We've added two new episodes, making this a five-part series that introduces the processes newly hired Federal civilians, military members, and contractors experience as part of the personnel vetting, or PV, process. You are about to listen to Episode 4: Continuous Vetting. We'll explore many aspects of why Continuous Vetting, or CV, exists, how it functions, and what your responsibility is within CV. At the conclusion of this episode, we invite you to listen to all webcast episodes if you haven't already.

**HOST:** Welcome to the WCDSE Personnel Vetting radio show, where we take your calls and answer all your PV-related questions! As always, I'm your host, Robert LaHart. Today, we have a new show and a new look and we're talking all about CV. Before I take calls, let me tell you what CV is. Recall from previous episodes we discussed the pre-investigation, investigation, and adjudication stages of the vetting process for new hires.

CV is the next step in the process. All trusted insiders must be evaluated on an ongoing basis. With full Trusted Workforce, or TW, implementation on the horizon, this applies across the board to everyone working for or on behalf of the Federal Government.

So why do we conduct CV? We conduct CV for many reasons. First, to promote early detection of potential issues and reduce risks. Second, to address concerning behaviors and perceived vulnerabilities as they emerge. In reality, the vetting process never actually ends for those working for or on behalf of the Government. It's not as simple as, "I got hired, they investigated me, granted my public trust or my national security eligibility, and now I'm done." The vetting is forever, ongoing.

Another thing to know is that CV is not one size fits all. Much like the investigation phase, the level of CV is determined by the position's designation or the sensitivity and risk that person's job duties pose. This in turn determines the specific conditions, information categories, and frequency of PV needed.

**HOST:** Let's take our first caller. Welcome to WCDSE. What CV questions do you have for us tonight?

**CALLER 1:** Hi Robert, this is John, and I'm just coming back to the Federal workforce after being gone for handful of years. When I left the Government, everyone was talking about continuous evaluation but now, I keep hearing about CV. They sound like the same thing to me.



Is CV different from continuous evaluation?

**HOST:** Thanks for calling, John, and what a great question.

They are similar but not the same thing. When continuous evaluation, or CE, began many years ago, trusted insiders would be registered in an automated system to run various checks in the background while they were still being re-investigated every 5 to 10 years.

CV is the evolution of that. CV now runs multiple automated records checks, or ARCs, and has replaced the requirement of formal re-investigations as individuals are evaluated on an ongoing basis for potential risk throughout their Federal affiliation. CV also encompasses a few other aspects like self-reporting and time- and event-driven information, but CE was the original starting point.

**CALLER 1:** So, what kind of information does CV pull from these automated checks?

**HOST:** CV pulls data from 7 categories: criminal, terrorism, foreign travel, financial activity, credit, public records, and eligibility.

**CALLER 1:** It's great that we are checking individuals' records more often. People don't always self-report and a lot can happen in 5 to 10 years that we should know about.

**HOST:** Exactly!

**HOST:** That's one of the biggest advantages to CV. We learn about issues in near-real time so your agency can address potential risks early, before someone loses their eligibility or becomes an insider threat. Individuals can be referred for help if they need it for issues like drug or alcohol problems and financial problems.

**CALLER 1:** Thank you for that clarification. I'm still not clear on a couple other things about CV. When do people get enrolled in CV?

**HOST:** Right now, security practitioners, usually security managers, are responsible for enrolling individuals in national security sensitive and non-sensitive public trust positions in CV. Once TW 2.0 is fully implemented, enrollment will happen automatically when the individual's background investigation begins. Individuals consent to CV enrollment by certifying the standard form or personnel vetting questionnaire.

**CALLER 1:** And who is enrolled in CV? I heard that only people with certain clearances are enrolled, and I also heard everyone is enrolled.

**HOST:** When TW 2.0 is fully implemented, all individuals, even those in low-risk positions, will be enrolled in CV and it will be done automatically. However, when implementation



began, it started with just the national security population. Currently, the entire national security population is enrolled, and we are starting to enroll the non-sensitive public trust population.

As part of Trusted Workforce 1.5, there are already about 4 million individuals in CV.

**CALLER 1:** OK. Well then, how do I know when an issue comes up from an ARC?

**HOST:** When a record check results in a finding, a DCSA CV analyst receives the alert.

The analyst validates the alert by verifying the personally identifiable information, or PII, matches that of the individual and that the alert is a new, not already known, issue.

Then, the analyst sends a notification of a CV report to DCSA Adjudications and the security management office of the individual that got the alert.

The investigative service provider, or ISP, may conduct issue resolution and engage the individual to obtain pertinent information concerning the alert.

One thing to keep in mind is that just because DCSA receives a CV alert doesn't automatically mean the individual is in trouble or will lose their security eligibility. CV alerts are a tool; they are a starting point for Government to investigate the issue further.

**CALLER 1:** Wow. That's good to know. One more question, what do I do if an alert is generated about me?

**HOST:** Each agency has their specific processes for responding to CV alerts.

In general, your DOW security manager will review the report and may gather more information from you about it. Based on the information you provide, they will make a recommendation to your local commander on whether to suspend your access.

Meanwhile, the ISP also reviews the CV alert. Depending on the seriousness of the issue, the ISP conducts issue resolution, obtains additional coverage as necessary, and passes the findings to an adjudicator.

The adjudicator applies the adjudication guidelines to determine if the incident can be effectively managed or mitigated. If unmitigated, your eligibility could be denied or revoked as part of security review proceedings, or SRP.

**CALLER 1:** Well, thank you for the information about CV, Robert. It helped a lot, but what's an SRP?

**HOST:** No problem, John, and thank you for calling.



SRP is previously known as due process and appeals. It is an administrative process to ensure a fair and impartial adjudication of facts and circumstances when an unfavorable trust determination is being considered. To learn about SRP, stay tuned for Episode 5 of the PV Process series where I interview a subject matter expert on the SRP process.

Before we take our next caller, let's hear a message from our sponsor.

**COMMERCIAL NARRATOR:** Would you like to learn more about Personnel Vetting? Do you have more questions about Continuous Vetting? Would you like more information about Trusted Workforce 2.0?

There's a toolkit for that!

Visit [cdse.edu](http://cdse.edu) and go to the Personnel Vetting Toolkit. There are job aids, games, shorts, videos, and even a Continuous Vetting tab! Don't delay, visit the PV toolkit today!

**HOST:** Welcome back. We have time for another caller. Hillary is on the line with some questions about CV and self-reporting. Hi Hillary, thank you for calling WCDSE.

**CALLER 2:** Hey Robert! I'm so glad you are talking about this topic. I just received my Secret eligibility, and I have lots of questions.

**HOST:** Congratulations!

**CALLER 2:** Thanks! Now that I've gone through adjudication and started in my new position, I was told I would be enrolled in CV and that I have to report certain things. Can you tell me what I am supposed to report? I can't remember everything from the brief I got.

**HOST:** Sure!

**HOST:** For everyone listening at home, do remember that during the beginning of today's episode, I mentioned that CV has evolved over time? CV is now comprised of not only ARCs, but also self-reporting!

In your case, it sounds like the security manager is remaining engaged with you and performed the required initial brief that informs you about the types of information you need to report.

You are required to self-report certain activities and conduct and promptly update your PVQ when a life event occurs. This can include many things, like getting married, having financial issues, or being charged with a crime. What you have to report is dependent on the risk and sensitivity level of the position you are in.



What do you remember from your brief?

**CALLER 2:** Well, I remember him saying I have to report trips to other countries.

**HOST:** That's right. So, all individuals, no matter their position and at all levels of eligibility, must report unofficial foreign travel before the trip. You also need to report any foreign contacts including personal- and business-related associations.

**CALLER 2:** If that is all I need to report, that doesn't seem too bad.

**HOST:** Well, that's not everything. We won't have enough time in this week's show to cover all the reporting requirements.

I recommend you read Security Executive Agent Directive, or SEAD, 3: Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position. It established the reporting requirements for all covered individuals. You can find that policy in the CDSE Personnel Vetting toolkit.

**CALLER 2:** My security manager told me that DCSA does automatic record checks and that I will be required to update my PVQ every five years. So, why should I self-report? It sounds like if something happens, the security manager will find out.

**HOST:** Well, there are a few reasons to self-report.

First, you demonstrate a level of trustworthiness and integrity by self-reporting and doing so is taken into consideration when an incident is reviewed.

Second, if you self-report, your agency may be able to provide or refer you for assistance. For example, if you report a problem with debt, then they can refer you to debt counseling before it becomes an issue that can impact your security eligibility.

Finally, you are required to self-report. If your security manager receives a CV alert of an incident that you did not report, your integrity, judgment, and reliability can be called into question and can result in administrative action.

**CALLER 2:** If something happens or changes, when am I required to self-report?

**HOST:** It depends on the event or the type of information.

If you are traveling to a foreign country for vacation, you need to report it at least two weeks before you go. This is called advanced reporting.

If there is a life event or incident, like getting married or getting arrested, report it as soon as possible within at least three days.



Sometimes, you will need to self-report in response to ad hoc information requests from your agency and as requested on a routine, periodic basis.

**CALLER 2:** So, if I have something to report, do I just call the security manager or my supervisor?

**HOST:** Your security manager should brief you on how to self-report per your agency's process.

You can self-report directly to your security manager, Facility Security Officer, or FSO, or agency.

You must also update sections and questions in your PVQ when a life event results in a change to a previously provided response. Once TW 2.0 is fully implemented, everyone will be able to self-report electronically, in the individual engagement platform, or IEP.

After you self-report, the security manager may ask for more information that is consistent with requirements of the Privacy Act.

**CALLER 2:** OK. Well, thank you for all the information, Rob. I took notes, but where can I find the list of things I'm supposed to self-report again?

**HOST:** You can go to the PV Toolkit on [cdse.edu](http://cdse.edu). You'll find SEAD 3: Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position and job aids that provide the CV information you need. There is also a CDSE job aid called Reporting Requirements Interactive Tool and a CDSE Short called Reporting Requirements-at-a-Glance.

**CALLER 2:** Thanks, Rob! I'll go check it out.

**HOST:** Thanks for calling.

**HOST:** One final note about self-reporting. Currently, only those in national security positions have self-reporting obligations. However, once TW 2.0 is fully implemented, all those working for or on behalf of the Federal Government will be required to self-report certain information. The future reporting requirements can be found in a policy called the Federal Personnel Vetting Management Standards Appendix C: Reporting Requirements for the Continuous Vetting of the Trusted Workforce. Once the policy is fully implemented, you can bet CDSE will update their website with a concise look at how the new policy impacts you.



**HOST:** Well folks, that's all the time we have today. Please check out Episodes One through Three, you can find them in the PV Toolkit. And stay tuned for our next webcast on SRP. Until then, keep doing your part to protect our people, our property, our information, and our mission. And remember, creating and maintaining a culture of trust is the shared responsibility of all of us. Have a great night!