NISPPAC Meeting March 18, 2026 Questions and Answers

Question from Nik A.: E-Verify offers an accepted electronic method to validate citizenship. Can DoD/DCSA speak on any consideration to update the 32 Page 31 CFR part 117.10 (C) NISPOM rule to validate original or certified copies of proof of citizenship to include language that supports a similar (if not the same) electronic method?

Answer: The answer is e-Verify is used for employment decisions but does not meet security requirements (neither personnel security policy nor the NISPOM permits this use). There are no plans to update the NISPOM but DCSA has put out this clarification to Industry:

The FSO or an authorized representative must verify the U.S. citizenship of every applicant. This verification must be based on the list of acceptable documents outlined in 32 CFR 117.10(c). It is crucial that applicants present either the original documents or certified copies for verification. To confirm the integrity of the documentation, the FSO or representative must view the documents in person. Prohibited Methods include using email, video technology, or any other remote method to view citizenship. In cases where operational needs prevent your FSO or representative from conducting the verification in person, you may authorize a trusted third party. Examples include notaries, outside legal counsel, or other government representatives. Before a third party can act on your behalf, your company must establish clear, written procedures. These procedures must ensure the third party is fully aware of their obligation to validate U.S. citizenship using only the authorized documents and must outline exactly how they will communicate the successful validation back to your FSO.

Question from Gretchen Alspaugh: Can we get some clarification on DISS and snipping/screenshots - in particular the VAR screen. We have had an issue where host sites aren't seeing VARs, don't go to page 2, or they were deleted by someone else in the host organization to put in a local database. When this became a prevalent issue, my security office started getting asked for snips as proof the VARs exist. Back in the JPAS days, this was strictly prohibited as it was a much more detailed page and the subject page has, understandably, always been off limits, but now there is much less information in VAR pages (e.g., no more SSN or DoDID listed). Some security offices are saying the same rules apply and others ask for the snips. What is the definitive ruling on this?

Answer: Per DISS Account Management Guidance, see section 5.8 Misuse of DISS: https://www.dcsa.mil/Portals/128/Documents/IS/DISS/NEW_DISS_Account_Request_Procedure.pdf, “Printing or taking screenshots of DISS data” is listed as a misuse of the system. It is recommended that users make use of several reports in the “JVS Reporting” capability:

- Subject Report - provides a roster of all subjects with an Owning or Servicing relationship with the user’s SMO.

- Hosting Visit Report - provides a roster of all subjects visiting the report user's SMOs within the selected start and end date. Visits may display that have a previous start date or a later end date than selected if those visits occur within the selected time frame.

Question from Joseph Whipp: Could you please go into greater detail, or readdress the comments about timelines and what candidates can see in eApp, [where individuals fill out the Questionnaire for National Background Investigation Services]? Are they able to see where they are in the process? Can they log back in after the [questionnaire] has been submitted?

Answer: It appears the question relates to both eApp and the Individual Engagement Platform (IEP).

Subjects will receive an email from eApp that will provide instructions for accessing their questionnaire (SF86 or PVQ A-B-C form) which includes a username and password that is system generated. Applicants receive a direct link in their eApp login email that they can track the status of their application through the Individual Engagement Platform (IEP).

The IEP is a live, applicant facing system that provides the individual with greater transparency. The launch was announced in a March 6th news article on DCSA.mil: https://www.dcsa.mil/About-Us/News/Article/Article/4424945/dcsa-launches-iep-status-tracker-to-enhance-transparency-and-customer-experience/ with an attached fact sheet with important instructions and details for FSOs.

Status tracker is an iterative roll out and some of the updates come in batch. For example, Applicant Editing the Form occurs overnight not real time. Everything past "submitted for processing" is greyed out. This is because we have to establish the connection with back-end systems (PIPS/IVM). The end state of status tracker expected in early FY27 will cover the end to end vetting process which includes tracking the investigation status, adjudication status and CV enrollment. All of the information provided on the IEP status tracker will also be available to the FSO through DISS-JVS. This is expected to provide the subject with more visibility into their status and reduce calls to their FSO for "where is my clearance?"

Subjects can log back into IEP anytime after their request is initiated, including after release to track their status. The future state of IEP is a suite of capabilities that will support collection of personnel vetting data from individuals. Functionality will include self-reporting, feedback loops, adjudicative correspondence, visit management and eInterviews.

Question from Douglas Cameron: With regards to the Individual engagement Platform (IEP), FSOs spend helping subjects properly report incidents with complete and accurate information and encourage them to include SEAD 4 mitigation that reduce the investigation and response requirements for any reports. Can you provide a quick overview of the next phase of the IEP (self-reporting) and how the workflow will incorporate the FSO? How will entities meet

requirements to report the same information to SAP & SCI & FSOs since per the IEP guidance, the FSOs are removed from the process?

Answer: The next feature of the IEP will be Self-Reporting which is expected in September. This capability will empower individuals to report required information and updates in accordance with the Federal Personnel Vetting Management Standards. Users will have a clear, categorized menu to report changes related to their personal information, foreign travel, financial status, and more. The forms are designed to be intuitive, easy to navigate and will offer a consistent template for subject entry.

There have been many questions concerning how this information will be presented to the Security Officer, HR Rep or FSO. It is not DCSA's intent to eliminate the SO/FSO from the self-reporting piece of IEP. We are tracking the self-report being presented in DISS-JVS for the Agency rep to review and take action on.

This has not been finalized yet and has not been built (thus the reason we do not have a screenshot of it). DCSA continues to work with PAC PMO, NISPPAC and agencies on how this will look and act to finalize this best practice.

The system will use the PVQ reporting format for collection and will follow form validation for the specific section being updated and the IEP Self Report will send a notification to DISS-JVS, and save the reported information to pre-fill future questionnaires, saving time and reducing errors for the next 5-year update.

Question from Douglas Cameron: How entities will meet their 32 CFR 117.8(c)(1)(i) requirements to report adverse information to host USG locations, if the FSO are not provided the information themselves?

Question from Douglas Cameron: How will entities will meet their 32 CFR 117.7(d) requirements to "report relevant and available information indicative of a potential or actual insider threat."

In effect DCSA, will get incomplete information from individuals without any additional information from the entity?

This is a great idea, with great potential, but the process should be similar the SF86 submissions with a review by the FSO.

Answer: Cleared entities will meet the requirements of 32 CFR 117.7(d) by establishing a formal, cross-functional Insider Threat Program that actively gathers, integrates, and analyzes data across the entire organization, resembling an intelligence-gathering hub. This structured requirement addresses the concern of incomplete reporting by ensuring that DCSA receives holistic, corporate-level assessments rather than relying solely on isolated, individual self-reports.

Question from Greg Pannoni: Recently I saw an article indicating that the latest TW 2.0 Quarterly Progress Report (QRP) was released and indicated, inter alia, that reform efforts would tackle updating meaningful performance metrics. One of those was a metric for rejection metrics. With that in mind, will DCSA begin reporting on PCL applicant rejection rates?

Answer: The Agency Performance Monthly Reporting Metrics currently include reporting on the percentage of deficient submissions. Based on the corrective action required, the outcome may lead to the rejection of the application. DCSA will continue to report metrics as required by the Federal Personnel Vetting Performance Management Standards.