

Answers to Questions Raised During the PSC Conference Call on OPM's Temporary Suspension of the e-QIP Security Clearance System and the Breach of OPM's SF-86 Data Base

e-QIP

Q1: Will personnel who are at the stage that the SF86, waivers and fingerprints are all submitted and it has now been handed over to OPM for the actual investigation, continue to be investigated, or will those also be shut down as OPM can't get at the info they need?

A1: As best we can determine, investigations that have already commenced will continue. However, at whatever point the investigative process requires access to e-QIP for any reason, it will come to a halt. Given e-QIP's central role, therefore, we are concerned that the clearance process will effectively grind to a halt and a backlog will quickly develop.

Q2: Who were the individuals that PSC wrote to and where do they work?

A2: PSC's July 1, 2015 letter was sent to OPM Director Katherine Archuleta and OMB Deputy Director Beth Cobert. You can find the text and the press release at: http://www.pscouncil.org/News2/NewsReleases/2015/Contractor_Community_Seeks_Answers_After_Sudden_e-QIP_Shutdown.aspx.

Q3: What is the extent of contractor organization legal liabilities? Is it all on the Govt?

A3: We don't provide legal advice and are unable to offer a definitive answer since it is not a well settled issue. In addition, we are, on some levels, in new territory. Clearly the government, as the holder of the personally identifiable information, has the principal responsibility. But that does not automatically mean that companies are entirely clear or that some affected employees won't attempt to tie the company to any impacts they experience. In short, while our belief is that the government is the responsible party, we cannot assert that companies will be free from any liabilities.

Q4: What about a periodic reevaluation (PR) that needs immediate initiation due to timing?

A4: If the PR requires access to e-QIP, the July 2, 2015 guidance from DNI and OPM implies that certain PRs can continue based on paper copies of the SF-86 questionnaire. Reports do suggest the administration plans to rely on the granting of temporary clearances as much as possible, but there are only a few entities that currently have the authority to grant clearances at all. So expanding that capacity will require a definitive and explicit policy action by the administration.

Answers to Questions Raised During the PSC Conference Call on OPM's Temporary Suspension of the e-QIP Security Clearance System and the Breach of OPM's SF-86 Data Base

Q5: Understanding the potential damage to individuals and employees, I also see potential damage(s) on current contracts where cleared people perform. Today's environment following Snowden, etc., has caused many clients and projects to push costs for escorts and clearances down onto contracts and contractors. Much of these costs and delays are due to the current delays in waiting for personnel clearances through OPM and e-QIP. This will only be further exacerbated with this new OPM policy and we really don't know if this 4-6 weeks is in fact accurate. Is there a sense on whether OPM might also issue guidance on these delays and potential cost impacts?

A5: *The July 2, 2015 guidance from DNI and OPM explicitly demurred contract performance questions to the contracting community. Addressing this issue is one of the reasons why we sent our letter on Wednesday, July 1st. E-QIP does have relevance, of course (and as you note), to more than personal security clearances. It also comes into play with facilities clearances, issuance of personal identity verification (PIV) cards and more. So the ripple effect of the suspension could be broad.*

Q6: With the shutdown, any e-QIP currently submitted in JPAS will be on hold correct?

A6: *Very helpful information from one member company security director (and former FSO) stated:*

JPAS allows FSO's to review completed E-QIP information for quality assurance purposes and then submit for processing. The day to day management of personnel security using JPAS (visit requests, granting access, submitting reports, etc.) should not have any tie to E-QIP. JPAS uses a strong security mechanism that is separate from E-QIP – access card with PKI cert and PIN. DMDC runs/hosts JPAS. Good resource for JPAS info: <https://www.dmdc.osd.mil/psawebdocs/docPage.jsp?p=JPAS>

Q7: In the past, hard copy SF-86s/SF-85Ps have been used. Does OPM have the capacity to do this now?

A7: *Unfortunately, we do not know the status of old paper records. In terms of creating new hard copies, it again depends on whether they need to enter e-QIP for any part of the process. The Director of National Intelligence (DNI) and OPM issued a memorandum on July 2nd announcing that paper copy SF-85's, SF-85P's and SF-86's will be used in the interim to initiate background investigations. However, this interim process is not authorized for TS, TS-SCI or Q Level information. Here's a link to the DNI-OPM memo:*

https://admin.govexec.com/media/gbc/docs/pdfs_edit/interim_procedures_during_the_temporary_suspension_of_e-qip.pdf

Answers to Questions Raised During the PSC Conference Call on OPM's Temporary Suspension of the e-QIP Security Clearance System and the Breach of OPM's SF-86 Data Base

Q8: Do we know what stages of the clearance process actually require access to e-QIP to proceed to the next step of the process?

A8: E-QIP is primarily used to provide the information used to initiate the background investigation, so it would appear that the biggest impact at this time will be on new requests for clearances and for investigations which have not yet commenced.

Q9: What should companies be thinking about doing in the near term?

A9: Here are helpful thoughts from a member company executive with regard to what companies might want to think about doing in the near term.

We recently sent an all hands message to our employees letting them know we are monitoring this closely and will keep them informed. We also provided a number of recommendations for credit monitoring, avoiding identity theft, and setting fraud alerts. We added in reminders on best practices for protecting their information in the electronic domain. We have not yet committed to paid credit monitoring pending clarifications from the Government on the extent of the impacts and what they intend to do.

SF-86 Data Breach

Q10: Has there been confirmation that contractor data has been breached or is that suspected, but unconfirmed at this time?

A10: There has been no formal confirmation, but given the numbers involved it is essentially a foregone conclusion that contractor data is among that which has been compromised. While OPM has identified 4 million current and former federal employees as having had their information taken during the breach of OPM's personnel data base, OPM has not yet identified the extent of the second data breach of security clearance (SF-86) information. This second breach has the potential to impact a large number of contractors and family members of personnel who have submitted SF-86 information as part of a background investigation. OPM has not identified a timetable as to when they will announce who has been compromised in this breach, with estimates being offered in the media of as many as 18M to 30M people. Further, OPM has not yet announced whether they will acknowledge any liability or offer any mitigation services to personnel compromised in this second breach. OPM has said that they will make an announcement on this soon, in the meantime, we do not know anything specific nor do we yet know the degree of exfiltration.