ISOO Special Briefing to the NISPPAC on OPM Breach

June 16, 2015

Notes:

- Will not address details of the breach, because this is an ongoing federal criminal investigation
- Why is ISOO involved?
    - Type of information compromised fits into the definition of CUI
    - Role of NISPPAC
- Affected individuals of first breach (federal employees) have been contacted, OPM is managing
- A separate event was detected at the end of last week, so multiple breaches are in play
- Second breach has FBI, DHS and OPM trying to determine nature and scope of breach which will eventually lead to an assessment of how many and who are impacted
- We will be getting regular updates through our NISP channels
- ISOO has briefed OPM on the function of the NISPPAC to let them know we have the capability to reach out to all of industry quickly
- Q: What would happen if individuals start to refuse to fill out their SF86 paperwork with the explanation that they do not feel their information will be kept secure?
    - A: This is very new and we have not yet had that happen. However, if this is becoming systematic, please push this up through ISOO and DSS and flag it as a consequence of the breach.
- Q: Do you have any information on timelines or sequencing of events in dealing with this breach?
    - A: Notification of affected individuals happening within 30 days is not necessarily bound by this timeframe, but they are trying to hit that mark. John Fitzpatrick has been called in about every third day for an update on the process. They are on board with the NISPPAC ability to notify industry of what is going on. This is so evolving, as soon as someone tries to pin down the scope, there is a reason to recalculate it.
- Q: I'm hoping that there is some special consideration being made as far as the authentication and the methods that the notifications are being made to the victims as this is a prime target for phishing?
    - A: Yes, we have already been learning this and this will continue to evolve if and when we notify the next grouping. We will be coming back and looking for feedback on how this process is going.
- Q: What happened that caused this and what can we do to ensure that this will not happen again?
    - A: That will not be a feature of this communication. That is being considered close hold because it is under federal investigation. Until it needs to be a part of this push notification communication process, I would not expect a lot on that.
- Q: Regarding the spear phishing, to mitigate that, would it be appropriate for individuals to be notified through their FSO of record?
    - A: Until we understand what has been compromised and what it constitutes, we cannot come up with a scheme for how to communicate this. There are so many unknowns currently in terms of scope and scale, it is too soon to know.

- Q: Has there been any consideration for credit monitoring and if so, who should be responsible for paying for those services?
    - A: Within the federal victims, those four million people are being offered those services. The notification process is to point them to the resource that OPM has set up and the costs will be borne by a mechanism that OPM will pay for. It is reasonable to expect that something like that would be offered to any affected folks in the subsequent breach. When the details of that are known, then they will determine how to notify.
- Q: In keeping with this topic, there will be some folks that want to lock their credit reports. How will government agencies be able to access records for folks that have locked credit reports and will the agencies give timeline considerations to the time it will take to deal with this?
    - A: This is more of a downstream item and something that will likely come up. We will need to address this as it comes up. We are very early in this process.
- Comment from DSS PR: We will be providing information on the dss.mil website, and will be using facebook and twitter to get communications out. But individual IS reps will not have many answers as there aren't many right now. We are in the very beginning stages right now.